École Doctorale de Géographie de Paris

Laboratoire Médiations – Sciences des lieux, sciences des liens

THÈSE

pour obtenir le grade de

DOCTEUR DE SORBONNE UNIVERSITÉ

Discipline : Géographie

Spécialité : Géopolitique

Présentée et soutenue publiquement par

Rémi LE GENISSEL

Le 2 juillet 2026

Cyberespace et standardisation des données géographiques numériques : un enjeu de la souveraineté nationale française (2021-2024)

Thèse réalisée sous la direction du

Professeur Philippe BOULANGER

Membres du jury :

Amaël CATTARUZZA ***rapporteur***
Fouad NOHRA ***rapporteur***
Edith FAGNONI ***présidente du jury***
Jean PEETERS ***examinateur***
Yann RICHARD ***examinateur***
Dimitri SARAFINOF ***invité***

CC BY NC ND

SOMMAIRE

Introduction.....8

Cadre théorique et méthodologique.....13

PREMIÈRE PARTIE — Comprendre la normalisation des informations géographiques numériques.....36

Chapitre I — Géopolitique et normalisation des données géographiques.....37
Chapitre II — L'écosystème de la normalisation des données géographiques.....128
Chapitre III — Les enjeux de la normalisation des données géographiques.....187
Conclusion de la partie 1.....216

DEUXIÈME PARTIE — Risque cyber et normalisation des données géographiques.....217

Chapitre IV — Les enjeux de la protection des données géographiques contre le risque cyber…..218
Chapitre V — Les infrastructures de données géographiques au cœur du risque cyber.....262
Chapitre VI — Les territoires au défi de la protection des données géographiques numériques….330
Conclusion de la partie 2.....390

TROISIÈME PARTIE — Normalisation géospatiale et recompositions géopolitiques.....393

Chapitre VII — Recomposition géopolitique et processus normatif : quel avenir pour la France et l'Europe ?.....396
Chapitre VIII — Le poids des nouvelles technologies dans la reconfiguration des rapports de pouvoir..... 467
Chapitre IX — Quel avenir pour la normalisation des données géographiques ?.....543
Conclusion de la partie 3.....591

Conclusion générale..... 593

Sources primaires.....601

Bibliographie.....622

Table des figures et cartes.....656

Annexes..... 659

Table des matières détaillée.....793

Remerciements

Tout d'abord, je tiens à remercier chaleureusement monsieur le professeur **Philippe Boulanger**, sans qui cette thèse n'aurait jamais pu avoir lieu. C'est en effet grâce à la confiance sans faille qu'il m'a accordée tout au long de l'écriture de cette thèse que j'ai pu réaliser ce travail sans encombre. Son encadrement exceptionnel m'a garanti un suivi particulièrement poussé tout au long des différentes étapes de ma recherche et de la rédaction de la présente thèse. Je tiens également à remercier profondément monsieur **Jean Peeters** et l'ensemble du personnel de la chaire de cybersécurité et souveraineté numérique du fonds de dotation de l'IHEDN. Le soutien financier du fonds de dotation de l'IHEDN pendant les trois premières années de ma recherche a en effet constitué une condition sine qua non de la réussite de cette thèse, qui n'aurait pu être entreprise sans cela. L'accompagnement scientifique de monsieur Peeters a par ailleurs été d'une aide précieuse tout au long de mon séjour au sein du fonds de dotation. Je tiens également à remercier monsieur et madame **Tortech** pour leur amitié de longue date et les conditions d'hébergement exceptionnelles qu'ils m'ont offertes tout au long de mes premières années de recherche à Paris. Je remercie également mon ami **Charles Marques** avec qui j'ai partagé toutes les tribulations d'un travail de recherche et dont j'ai hâte de pouvoir lire le travail que je sais être exceptionnel. Je voudrais également remercier profondément monsieur **Dimitri Sarafinof** et monsieur **Alain Zumsteeg** qui m'ont ouvert les portes des instances de normalisation internationales (civils et militaires respectivement), sans lesquels je n'aurais jamais pu espérer mener à bien ce travail de recherche, et que j'ai la chance aujourd'hui d'avoir comme collègue au sein de l'équipe normalisation de l'IGN. Je souhaite également remercier madame la **Colonelle Isabelle Messa** qui m'a aidé à mener à bien mes recherches au sein des instances de normalisation militaires. Je voudrais également remercier l'ensemble du personnel de l'IGN dont les noms seraient trop nombreux à citer ici, qu'il s'agisse de ceux qui ont bien voulu se plier à l'exercice de l'entretien dans le but de m'éclairer sur les enjeux de mon sujet de thèse, que ceux qui partagent aujourd'hui mon quotidien professionnel au sein de l'Institut et dont le professionnalisme et l'amitié me sont précieux. Il me faut également remercier ici toutes les personnes, civils, comme militaires, qui ont bien voulu répondre à mes questions et m'aider tout au long de mon parcours de recherche pour mieux comprendre les enjeux de la standardisation des données géographiques numériques. Enfin, ces remerciements ne sauraient être complets sans ceux que j'adresse à ma famille, à mes amis et à ma compagne **Julie Portier** qui m'ont soutenu et accompagné tout au long de ce travail de recherche et dont le soutien moral fut inestimable.

Introduction

Le 24 février 2022, lorsque les forces armées russes franchissent les frontières ukrainiennes, les systèmes de positionnement par satellite, les cartes numériques et les réseaux de communication géospatiale deviennent instantanément des enjeux de premier plan pour l'ensemble des belligérants. Dans les heures qui suivent l'invasion, des cyberattaques massives ciblent les infrastructures de données géographiques ukrainiennes, tandis que des tentatives de brouillage GPS perturbent les systèmes de navigation civils et militaires sur l'ensemble du territoire[1]. Cette guerre, qui peut être qualifiée de premier conflit de haute intensité de l'ère numérique, révèle avec une acuité sans précédent la dimension stratégique des données géographiques numériques et, par extension, des normes techniques qui en régissent la production, l'échange et la sécurisation. En effet, maîtriser l'information géospatiale ne relève pas seulement de la connaissance du terrain, c'est avant tout exercer une forme de souveraineté sur l'espace numérique lui-même.

Cette réalité contemporaine s'inscrit dans une longue trajectoire historique qui lie profondément la production cartographique à l'exercice de la puissance étatique. Depuis la création du Dépôt de la Guerre en 1688[2], qui visait à rassembler l'ensemble des cartes utiles à la défense du royaume de France, jusqu'à l'adoption du système métrique en 1791, première entreprise mondiale de normalisation des mesures géographiques, l'État français a très tôt perçu la maîtrise du savoir géographique comme une prérogative régalienne. Comme le souligne Philippe Boulanger, la *« codification et l'uniformisation des cartes à partir des travaux de la commission de topographie, créée en 1802 »*[3], ainsi que *« l'adoption de signes conventionnels »* et de projections normalisées ont participé de *« la tendance à la rationalisation des modes de production centralisée »*[4] de l'information géographique militaire[5]. La numérisation de ces données depuis les années 1990, puis leur intégration au cyberespace mondial, n'a fait que renforcer cette dimension stratégique tout en en complexifiant considérablement les enjeux. Les données géographiques numériques circulent désormais sur des réseaux transnationaux, sont

---

1 Sur les cyberattaques contre l'Ukraine dans les premières heures de l'invasion, voir notamment : Cattaruzza Amaël, Music Maylis, « La guerre en Ukraine, premier conflit de haute intensité à l'ère numérique », *Hérodote*, n° 186-187, 2022, pp. 7-24 ; Sur les tentatives de brouillage GPS, voir : Humphreys Todd E., « Statement on the Vulnerability of Civil GPS to Spoofing Attacks », *U.S. House of Representatives Committee on Homeland Security*, 2022.

2 Sur la création du Dépôt de la Guerre en 1688, voir : Berthaut Henri-Marie-Auguste, *Les ingénieurs géographes français (1624-1831)*, Paris, Imprimerie du Service géographique, 1902.

3 Boulanger Philippe, *La géographie, reine des batailles*, Paris, Perrin, 2020, 432 p.

4 *Ibid*

5 Sur l'adoption du système métrique comme première normalisation mondiale des mesures, voir : Alder Ken, *The Measure of All Things: The Seven-Year Odyssey and Hidden Error That Transformed the World*, New York, Free Press, 2002.

traitées par des algorithmes développés aux quatre coins du globe, et leur interopérabilité dépend de normes élaborées dans des arènes internationales où se jouent des rapports de force géopolitiques majeurs.

La présente thèse porte sur les processus de standardisation des données géographiques numériques et leurs implications pour la souveraineté nationale française. Par données géographiques numériques, est entendu ici l'ensemble des informations géoréférencées produites, stockées et diffusées sur des supports informatiques, qu'il s'agisse de cartes topographiques, d'images satellitaires, de modèles numériques de terrain, métadonnées géospatiales, ou encore données de positionnement issues des systèmes de navigation par satellite. Par standardisation ou normalisation, termes qui sont ici employés de manière interchangeable, est désigné, selon la définition de l'Organisation Internationale de Normalisation (ISO), *« l'activité consistant à établir, au regard de problèmes réels ou potentiels, des modalités d'utilisation commune et répétée, visant à atteindre le degré de fonctionnement optimal dans un contexte donné »*[6]. Enfin, la notion de souveraineté est ici entendue dans son acception géopolitique : la capacité d'un État à exercer un contrôle effectif sur un domaine donné, en l'occurrence, les infrastructures informationnelles géographiques, et à défendre ses intérêts dans les arènes où se définissent les règles qui encadrent ce domaine.

Le champ géographique de cette recherche englobe plusieurs échelles emboîtées. En premier lieu l'échelle internationale, où se développent les normes au sein d'organisations telles que l'Organisation internationale de normalisation (ISO)[7], l'Organisation hydrographique internationale (OHI)[8] ou le consortium Open Geospatial Consortium (OGC)[9]. L'échelle européenne d'autre part, structurée autour du Comité européen de normalisation (CEN)[10] et de la directive INSPIRE[11], l'échelle atlantique et militaire, avec le Defence Geospatial Information Working Group (DGIWG)[12] et

---

[6] L'Organisation internationale de normalisation (ISO) définit la norme comme « l'activité consistant à établir, au regard de problèmes réels ou potentiels, des modalités d'utilisation commune et répétée, visant à atteindre le degré de fonctionnement optimal dans un contexte donné ». Source : ISO, *Guide ISO/IEC 2:2004 – Normalisation et activités connexes – Vocabulaire général*.

[7] Sur le TC 211 de l'ISO, voir : ISO/TC 211, *Geographic information/Geomatics – Business Plan*, 2023. La thèse analyse en détail ce comité technique et ses groupes de travail.

[8] Organisation hydrographique internationale (OHI), fondée en 1921, siège à Monaco. Voir : *https://iho.int*. La thèse examine en détail le rôle de l'OHI dans la normalisation des données hydrographiques.

[9] Open Geospatial Consortium (OGC), consortium international fondé en 1994. Voir : *https://www.ogc.org*.La thèse consacre des développements substantiels à l'OGC et à ses normes (WMS, WFS, API, etc.).

[10] Comité européen de normalisation (CEN) et Comité européen de normalisation électrotechnique (CENELEC). Voir : *https://www.cencenelec.eu*.

[11] Directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE). *Journal officiel de l'Union européenne*, L 108, 25 avril 2007.

[12] Defence Geospatial Information Working Group (DGIWG), fondé en 1983. Voir : *https://dgiwg.org*.

l'Organisation du Traité de l'Atlantique Nord (OTAN)[13], et enfin l'échelle nationale française, articulée autour de l'Association française de normalisation (AFNOR)[14], du Conseil national de l'information géolocalisée (CNIG)[15] et de l'Institut national de l'information géographique et forestière (IGN)[16]. Cet aspect multiscalaire de l'analyse est constitutif de l'objet d'étude de cette thèse. En effet, les normes géospatiales se développent dans un système de « vases communicants » où les décisions prises à un échelon se répercutent nécessairement sur les autres.

La délimitation temporelle retenue (2021-2024), correspond à une période charnière dans l'histoire de la normalisation géospatiale. Elle s'ouvre avec la publication du décret du 10 novembre 2021 réformant le système français de normalisation[17] et la refondation du CNIG sous l'impulsion du rapport parlementaire Faure-Muntian intitulé *Les données géographiques souveraines*[18], et elle s'achève au moment où les travaux de terrain de cette thèse ont pris fin, alors que se dessinent les contours d'une possible fragmentation normative mondiale sous l'effet des rivalités sino-américaines. Cette période concentre ainsi des dynamiques de recomposition institutionnelle à l'échelle nationale et des tensions géopolitiques croissantes à l'échelle internationale.

Ainsi, la normalisation est souvent perçue comme un processus éminemment technique, voire apolitique, relevant de la seule expertise des ingénieurs. Cette représentation, encore dominante dans le sens commun, masque la réalité d'un champ traversé par des logiques de pouvoir, des rivalités économiques et des stratégies étatiques. Comme le soulignait l'économiste Olivier Favereau, la norme constitue un *« dispositif cognitif collectif »*[19] qui, bien au-delà de sa fonction technique, participe à structurer les anticipations mutuelles des acteurs et à façonner les trajectoires technologiques futures. Dans le domaine des données géographiques numériques, ces enjeux revêtent une dimension particulière. Il ne s'agit pas seulement de garantir la compatibilité de produits industriels, mais de définir les règles qui régissent la représentation, l'échange et la protection d'informations touchant directement à la connaissance et à la défense du territoire.

---

[13] Sur le rôle de l'OTAN en matière de normalisation géospatiale, voir notamment : NATO, *MC 0296/3 – NATO Geospatial Policy*, 2011 ; NATO, *NATO Geospatial Information Framework*, 2018.

[14] Association française de normalisation (AFNOR), créée en 1926. Voir : *https://www.afnor.org*.

[15] Conseil national de l'information géolocalisée (CNIG). Décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géolocalisée, modifié par le décret n° 2022-1204 du 30 août 2022. Voir : *https://cnig.gouv.fr*. La thèse analyse en détail l'évolution institutionnelle du CNIG.

[16] Institut national de l'information géographique et forestière (IGN). Voir : *https://www.ign.fr*. L'IGN est un acteur central de la thèse, analysé sous l'angle de son rôle dans la normalisation.

[17] Décret n° 2021-1473 du 10 novembre 2021 relatif à la normalisation. *Journal officiel de la République française*, 12 novembre 2021.

[18] Faure-Muntian Valéria, *Rapport d'information sur les données géographiques souveraines*, Assemblée nationale, n° 1178, 17 juillet 2018.

[19] Favereau Olivier, « Marchés internes, marchés externes », *Revue économique*, vol. 40, n° 2, 1989, pp. 273-328.

De cette tension entre la dimension technique et la dimension géopolitique de la normalisation découle la problématique principale de cette thèse qui s'exprime comme suit :

Dans quelle mesure la standardisation des données géographiques numériques constitue-t-elle un enjeu de souveraineté pour la France à l'aune de l'accélération des menaces cyber, et selon quelles modalités l'État français peut-il défendre ses intérêts dans un écosystème normatif de plus en plus internationalisé et compétitif ?

Cette interrogation générale se décline en plusieurs questions subsidiaires auxquelles cette thèse va chercher à répondre. Premièrement, quelles sont les spécificités des données géographiques numériques qui en font un objet stratégique distinct des autres catégories de données ? Comment s'organise l'écosystème international de la normalisation géospatiale, quels rapports de force le traversent, et quelle place y occupe la France ? Quels sont les enjeux propres aux différents acteurs français (civils et militaires, publics et privés), engagés dans ces processus normatifs ? Comment les mutations technologiques en cours, notamment l'émergence de l'informatique quantique et de l'intelligence artificielle, redéfinissent-elles les enjeux de cybersécurité et de normalisation des données géospatiales ? Enfin, quelles stratégies la France peut-elle déployer pour préserver ses marges d'autonomie face au risque d'une fragmentation normative mondiale ?

Afin de répondre aux questionnements soulevés par ce travail de thèse, la démonstration s'articule en trois parties qui permettent de saisir progressivement les enjeux géopolitiques de la normalisation des données géographiques numériques pour la souveraineté nationale française.

La première partie de cette thèse vise à poser les fondements nécessaires à la compréhension de cet objet d'étude. Elle vise d'abord à déconstruire l'idée reçue selon laquelle la normalisation serait un processus purement technique et apolitique, en retraçant l'histoire des rivalités de pouvoir qui traversent ce domaine depuis son institutionnalisation au début du XXe siècle, et en situant la place singulière de la France dans cet environnement. Elle examine ensuite les spécificités de la normalisation des données géographiques numériques et le lien qui les unit désormais à la cybersécurité. L'analyse se poursuit par une cartographie de l'écosystème international de la normalisation géospatiale, tant civil que militaire, mettant en lumière les organisations en présence et les rapports de force qui les structurent. Enfin, cette partie identifie les enjeux propres aux différents acteurs impliqués et la position des acteurs français dans ce paysage institutionnel complexe.

La deuxième partie descend à l'échelle nationale pour analyser les dynamiques territoriales de la normalisation géospatiale en France. Elle examine la gouvernance multiniveau de l'information géographique, les tensions entre centralisation étatique et autonomie des collectivités, ainsi que les

défis de l'interopérabilité entre la multitude de plateformes géographiques locales et les projets nationaux. Cette partie met également en évidence les vulnérabilités croissantes liées à la cybersécurité, particulièrement aiguës pour les collectivités territoriales qui manquent de moyens et de compétences spécialisées. Elle interroge les modèles de souveraineté sur les données géographiques, entre contrôle étatique, ouverture aux acteurs privés et logiques de partage, et analyse les enjeux juridiques qui entourent la protection de ces données stratégiques.

La troisième partie ouvre une perspective prospective en interrogeant l'avenir de la normalisation géospatiale à l'aune des bouleversements géopolitiques contemporains. Elle analyse d'abord les recompositions de puissance qui affectent le processus normatif international, notamment la contestation de l'hégémonie occidentale par la Chine et les fractures croissantes de la gouvernance mondiale des normes. Elle examine ensuite l'impact des technologies émergentes, comme l’intelligence artificielle, la blockchain, les jumeaux numériques, ou encore la cryptographie post-quantique, sur les référentiels techniques et les nouvelles rivalités qu'elles engendrent. Enfin, elle explore trois scénarios potentiels pour l'avenir de la normalisation : une fragmentation normative par blocs géopolitiques, une convergence multilatérale préservant l'interopérabilité mondiale, ou l'émergence d'une troisième voie européenne fondée sur des standards ouverts, mais souverains. Une attention particulière a été portée dans cette partie, ainsi que dans l’ensemble de ce travail aux implications pour la normalisation de défense et aux stratégies d'influence que la France peut déployer pour tenir son rang dans la compétition normative.

Cadre théorique et méthodologique

La présente section vise à expliciter et à approfondir le cadre théorique qui sous-tend l'ensemble de cette recherche. Elle répond à une triple exigence. Il s'agit tout d'abord, d'ancrer rigoureusement cette démarche dans le champ de la géopolitique tout en en problématisant les concepts clés, de définir avec précision la notion de « souveraineté numérique » qui constitue le cœur de sa problématique, et d'inscrire cette analyse dans le dialogue avec la littérature en économie politique de la normalisation. Cette explicitation théorique est d'autant plus nécessaire que l'objet d'étude de cette thèse, les normes techniques régissant les données géographiques numériques, se situe à l'intersection de plusieurs disciplines qui mobilisent des cadres conceptuels distincts.

1. Ancrage géopolitique : de l'espace physique au cyberespace

1.1. La géopolitique comme étude des rivalités de pouvoir sur les territoires

Ce travail de recherche s'inscrit dans le champ de la géopolitique, tel qu'il a été refondé en France par Yves Lacoste à partir des années 1970. Dans son ouvrage fondateur, *La géographie, ça sert d'abord à faire la guerre*, Lacoste opérait une double rupture. Il rompait non seulement avec la géographie vidalienne, accusée d'avoir dépolitisé le savoir géographique en le réduisant à une description érudite des régions, et avec le tabou qui, depuis la Seconde Guerre mondiale, frappait le terme même de « géopolitique », associé aux dérives du nazisme[20]. Contre ces deux écueils, Lacoste proposait de réhabiliter une géographie consciente de ses enjeux politiques et de ses usages stratégiques.

La définition de la géopolitique qu'il propose est désormais classique. Il s'agit de l'étude des « *rivalités de pouvoir sur des territoires* »[21]. Cette définition appelle plusieurs remarques. Premièrement, elle place les rivalités au centre de l'analyse, la géopolitique ne s'intéresse pas aux territoires comme objets inertes, mais comme enjeux de conflits entre acteurs aux intérêts divergents. Deuxièmement, ces rivalités portent sur le pouvoir, entendu ici non pas seulement comme domination coercitive, mais plus largement comme la capacité d'agir sur le monde et sur les autres acteurs,

[20] Lacoste Yves, *La géographie, ça sert d'abord à faire la guerre*, Paris, Maspero, 1976 (réédition La Découverte, 2014), p.9

[21] Lacoste Yves, « La géographie », in Badie Bertrand, Smouts Marie-Claude (dir.), *Le retournement du monde. Sociologie de la scène internationale*, Paris, Presses de Sciences Po/Dalloz, 1992, p. 33.

rejoignant ici la définition de la puissance que donnait Raymond Aron[22] vingt ans plus tôt. Troisièmement, ce pouvoir s'exerce sur des territoires, c'est-à-dire des espaces appropriés, délimités, chargés de significations et d'enjeux pour les acteurs qui s'y confrontent.

Cependant, une question fondamentale pour cette étude demeure, cette définition, forgée pour rendre compte des conflits territoriaux classiques (guerres, frontières, revendications séparatistes), peut-elle être transposée au domaine des normes techniques régissant les données géographiques numériques ? La question mérite d'être posée explicitement, car la transposition n'a rien d'évident. Les normes techniques ne sont pas des territoires au sens traditionnel du terme, ces dernières ne s'inscrivent pas dans un espace physique délimité par des frontières. Pourtant, cette thèse soutient que l'approche géopolitique reste pertinente pour les analyser, à condition d'élargir la notion de territoire pour y inclure les espaces immatériels du cyberespace.

1.2. L'extension de la géopolitique au cyberespace

Depuis les années 2010, un courant de recherche s'est développé autour de la « géopolitique du cyberespace », dont Frédérick Douzet est en France l'une des principales représentantes. Dans un article programmatique, elle définissait ainsi le projet : *« La géopolitique peut contribuer à la compréhension du cyberespace en analysant les rivalités de pouvoir pour le contrôle de l'espace numérique ou par l'espace numérique »*[23]. Cette définition distingue donc deux types de rivalités, celles qui visent le contrôle *du* cyberespace (les infrastructures, les protocoles, les données) et celles qui s'exercent *par* le cyberespace (les cyberattaques, l'influence informationnelle, l'espionnage numérique).

Amaël Cattaruzza, dans ses travaux sur la « géopolitique des données numériques », a prolongé cette réflexion en soulignant que *« les données numériques constituent désormais un enjeu géopolitique à part entière, au même titre que les ressources naturelles ou les positions stratégiques »*[24]. Cette proposition est importante pour notre recherche. En effet, elle établit que les données, et par extension, les normes qui régissent leur production, leur circulation et leur exploitation, peuvent être analysées comme des objets géopolitiques.

Toutefois, l'extension de la géopolitique au cyberespace ne va pas sans difficultés conceptuelles. La principale tient à la nature même de l'espace numérique. Contrairement à l'espace géographique physique, le cyberespace n'est pas donné d'avance, il est construit par les infrastructures techniques

[22] Aron Raymond. *Paix et guerre entre les nations*, Paris, Calmann-Lévy, 1962.

[23] Douzet Frédérick, « La géopolitique pour comprendre le cyberespace », *Hérodote*, n° 152-153, 2014, p. 4.

[24] Cattaruzza Amaël, *Géopolitique des données numériques : Pouvoir et conflits à l'heure du Big Data*, Paris, Le Cavalier Bleu, 2019, p. 15.

(câbles, serveurs, satellites), les protocoles de communication (TCP/IP, HTTP), les logiciels et les données qui y circulent. Comme l'ont souligné Douzet et Desforges, « *le cyberespace est un espace dual, qui articule une dimension matérielle (les infrastructures) et une dimension immatérielle (les couches logiques et sémantiques)* »[25].

Cette dualité a des implications importantes pour l'objet d'étude de cette thèse. Les données géographiques numériques occupent dans ce dispositif une position particulière, elles sont à la fois un objet du cyberespace, et une représentation de l'espace géographique physique. Elles instituent ainsi un lien ontologique entre les deux dimensions, à travers les données géographiques numériques, le cyberespace et l'espace physique s'interpénètrent. Cette interpénétration fait des normes qui régissent ces données un objet géopolitique particulièrement sensible, puisqu'elles touchent à la fois à la maîtrise du cyberespace et à la représentation du territoire physique.

1.3. La norme comme territoire : vers une géopolitique des espaces normatifs

Peut-on parler de « territoire » à propos des normes techniques ? L'emploi du terme de territoire concernant les normes techniques ne va pas de soi, mais il éclaire ici utilement les enjeux entourant les normes. Un territoire, au sens géopolitique, n'est pas seulement une étendue physique, c'est un espace approprié, c'est-à-dire investi par des acteurs qui y exercent un pouvoir, y projettent des représentations et y défendent des intérêts. En ce sens, l'espace normatif, qui est constitué par l'ensemble des règles, standards et protocoles qui régissent un domaine technique, peut être analysé comme un territoire.

Tout d'abord, l'espace normatif est délimité. Les normes définissent ce qui est conforme et ce qui ne l'est pas, ce qui est interopérable et ce qui ne l'est pas. Ces frontières ne sont pas physiques, mais elles n'en sont pas moins réelles. En effet, un système qui n'implémente pas correctement une norme se trouve exclu de l'écosystème qu'elle structure. De plus, l'espace normatif est approprié. Les acteurs qui participent à l'élaboration des normes, qu'il s'agisse des États, des entreprises, des organisations internationales, ou encore des communautés d'experts, y investissent des ressources considérables et cherchent à y faire prévaloir leurs intérêts. Enfin, l'espace normatif est conflictuel. Les processus de normalisation sont traversés par des rivalités entre acteurs aux visions et aux intérêts divergents. Ces rivalités portent sur le contenu des normes, mais aussi sur les règles du jeu qui déterminent comment elles sont élaborées et qui peut y participer.

[25] Douzet Frédérick, Desforges Alix, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », *Hérodote*, n° 177-178, 2020, pp. 3-15.

Cette conception de la norme comme territoire permet de comprendre pourquoi les États s'intéressent de plus en plus aux processus de normalisation. Comme dans les conflits territoriaux classiques, il s'agit de contrôler un espace, d'y exercer une influence, d'en définir les règles. La différence est que ce territoire n'est pas géographique au sens physique, mais normatif, c'est l'espace des règles techniques qui façonnent les possibilités d'action des acteurs économiques, sécuritaires et politiques.

2. La souveraineté numérique : clarification conceptuelle

2.1. La souveraineté : un concept polysémique

Le concept de souveraineté est au cœur de la problématique de ce travail de thèse, mais il est également l'un des plus polysémiques du vocabulaire politique. Stephen Krasner, dans son ouvrage *Sovereignty: Organized Hypocrisy*, distinguait quatre acceptions de la souveraineté[26] : la souveraineté domestique (la capacité à exercer l'autorité au sein d'un territoire), la souveraineté d'interdépendance (la capacité à contrôler les flux transfrontaliers), la souveraineté juridique internationale (la reconnaissance mutuelle des États comme entités juridiques égales), et la souveraineté westphalienne (l'exclusion de toute autorité externe dans les affaires intérieures d'un État).

Ces distinctions, forgées pour analyser la souveraineté étatique traditionnelle, ne se transposent pas mécaniquement au domaine numérique. La souveraineté, dans son acception classique héritée de Jean Bodin, désigne *« la puissance absolue et perpétuelle d'une République »*[27], c'est-à-dire la capacité d'un pouvoir politique à édicter des règles sur un territoire délimité, sans être soumis à une autorité supérieure. Or, le cyberespace se caractérise précisément par la difficulté à y appliquer les catégories territoriales classiques. En effet, les données circulent à travers les frontières, les infrastructures sont souvent contrôlées par des acteurs privés transnationaux, et les normes techniques qui régissent cet espace sont élaborées dans des arènes internationales où la voix des États n'est qu'une parmi d'autres.

---

[26] Krasner Stephen D., *Sovereignty: Organized Hypocrisy*, Princeton, Princeton University Press, 1999, pp. 3-4.

[27] Bodin Jean, *Les Six Livres de la République*, Paris, 1576, Livre I, chapitre VIII : « La souveraineté est la puissance absolue et perpétuelle d'une République ».

2.2. Trois conceptions de la souveraineté numérique

La notion de « souveraineté numérique », apparue dans le débat public au cours des années 2010, fait l'objet d'interprétations divergentes. À la suite des travaux tels que ceux de Pierre Bellanger[28], de Maylis Music[29], ou encore de Luciano Floridi[30] et des documents stratégiques de l'Union européenne[31], trois conceptions de la souveraineté numérique se distinguent, qui correspondent à trois manières d'articuler la notion classique de souveraineté aux réalités du cyberespace.

La première conception peut être qualifiée de souveraineté numérique territorialisée. Elle transpose au cyberespace le modèle westphalien en postulant que l'État doit exercer sur les données et les infrastructures numériques situées sur son territoire le même type de contrôle qu'il exerce sur son territoire physique. Cette conception se traduit par des politiques de localisation des données (obligation de stocker certaines données sur le territoire national), de contrôle des équipements de réseau (interdiction de fournisseurs étrangers jugés menaçants), et de régulation des contenus circulant sur Internet. Elle est particulièrement associée aux positions de la Russie et de la Chine, qui promeuvent le concept de « cybersouveraineté » dans les enceintes internationales[32].

La deuxième conception est celle de la souveraineté numérique comme autonomie stratégique. Elle met l'accent non pas sur le contrôle territorial, mais sur la capacité d'un État (ou d'un ensemble d'États, comme l'Union européenne) à agir de manière autonome dans l'espace numérique, c'est-à-dire sans dépendre de technologies, de services ou de normes contrôlés par des puissances étrangères. Cette conception, dominante dans le discours européen depuis la fin des années 2010, ne vise pas à fragmenter Internet ou à ériger des frontières numériques, mais à réduire les dépendances et à préserver des marges de manœuvre[33]. Elle se traduit par des politiques de soutien aux champions industriels européens, de promotion des logiciels libres et des standards ouverts, et de participation active aux instances de normalisation internationale.

Enfin, la présente thèse invite également à considérer une troisième conception de la souveraineté numérique, celle de la souveraineté numérique comme capacité normative. Cette

---

28 Bellanger Pierre, *La souveraineté numérique*, Paris, Stock, 2014, p. 12.

29 Music Maylis, « La souveraineté numérique : un concept en construction », *Études de l'IFRI*, Focus stratégique n° 115, mars 2023, pp. 8-12.

30 Floridi Luciano, « The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU », *Philosophy & Technology*, vol. 33, 2020, pp. 369-378.

31 Commission européenne, *Façonner l'avenir numérique de l'Europe*, COM(2020) 67 final, 19 février 2020, p. 2.

32 Couture Stéphane, Toupin Sophie, « What does the notion of 'sovereignty' mean when referring to the digital? », *New Media & Society*, vol. 21, n° 10, 2019, pp. 2305-2322.

33 Pohle Julia, Thiel Thorsten, « Digital sovereignty », *Internet Policy Review*, vol. 9, n° 4, 2020, pp. 1-19.

conception déplace le regard des infrastructures et des données vers les règles qui les régissent. Dans cette perspective, est souverain celui qui peut participer à la définition des normes, techniques, juridiques, et éthiques, qui structurent l'espace numérique. La souveraineté n'est donc pas seulement affaire de contrôle territorial ou d'autonomie industrielle, elle est aussi, et peut-être surtout, affaire d'influence dans les arènes où se négocient les standards de demain. Cette conception est particulièrement pertinente pour l'objet ici étudié, car elle implique que la participation aux processus de normalisation internationale constitue une dimension essentielle de la souveraineté numérique.

2.3. Définition retenue pour la présente recherche

Pour les besoins de cette recherche, est retenue une définition de la souveraineté numérique qui articule les trois dimensions précédentes, tout en mettant l'accent sur la dimension normative. La souveraineté numérique est ici définie comme la capacité d'un État (ou d'un ensemble d'États) à :

- Exercer un contrôle effectif sur les infrastructures numériques critiques situées sur son territoire ou essentielles à son fonctionnement.
- Disposer d'une autonomie technologique suffisante pour ne pas dépendre exclusivement de solutions contrôlées par des puissances étrangères.
- Participer de manière significative aux processus de normalisation internationale qui définissent les règles du jeu dans le domaine numérique.

Cette définition présente plusieurs intérêts pour cette thèse. Elle évite l'écueil d'une conception purement défensive de la souveraineté, qui réduirait celle-ci au contrôle territorial et à la fermeture. Elle reconnaît la dimension internationale et coopérative de la souveraineté numérique. Dans un monde interconnecté, l'autonomie se construit aussi par la participation aux instances de gouvernance mondiale. Enfin, elle place au centre de l'analyse la question des normes, qui constitue le cœur de ce travail.

3. L'économie politique de la normalisation : cadre analytique

3.1. La normalisation comme gouvernance privée transnationale

L'étude de la normalisation a fait l'objet d'une littérature abondante en économie politique internationale. L'ouvrage de Tim Büthe et Walter Mattli, *The New Global Rulers,* constitue une référence incontournable. Les auteurs y analysent la normalisation comme une forme de *« gouvernance privée transnationale »*[34], c'est-à-dire un mode de régulation de l'économie mondiale qui échappe largement aux États pour être pris en charge par des acteurs privés, entreprises, associations professionnelles, organisations de normalisation. Jean-Christophe Graz, dans *La gouvernance de la mondialisation*, a prolongé cette analyse en montrant comment la normalisation s'inscrit dans une transformation plus large des modes de régulation de l'économie mondiale, caractérisée par le brouillage des frontières entre public et privé, national et international[35].

Cette littérature met en lumière plusieurs caractéristiques des processus de normalisation contemporains. Tout d'abord, leur internationalisation. Les normes techniques sont de plus en plus élaborées dans des arènes internationales (ISO, OGC, W3C, etc.) plutôt qu'au niveau national. Également, leur privatisation. En effet, les acteurs privés, les entreprises, mais aussi les organisations de normalisation elles-mêmes jouent un rôle croissant dans l'élaboration des normes, tandis que la capacité des États à orienter les processus s'en trouve remis en cause. Enfin, leur technicisation, les débats normatifs sont présentés comme purement techniques, ce qui tend à masquer les enjeux de pouvoir et les choix politiques qu'ils engagent[36].

Comme le soulignent Brunsson et Jacobsson, *« nous vivons dans un monde de standards »* où les normes techniques structurent de manière croissante les pratiques économiques, sociales et politiques[37]. Cette omniprésence des standards pose la question de leur légitimité démocratique. De fait, les standards sont largement élaborés dans des arènes d'experts, alors même qu'ils impactent directement ou indirectement la vie de millions de personnes. Comment s'assurer alors de la participation d'un panel d'acteurs suffisamment vaste pour garantir une représentation démocratique dans ces instances de normalisation ?

---

[34] Büthe Tim, Mattli Walter, *The New Global Rulers: The Privatization of Regulation in the World Economy*, Princeton, Princeton University Press, 2011, p. 3.

[35] Graz Jean-Christophe, *La gouvernance de la mondialisation*, Paris, La Découverte, 2013, p. 78.

[36] Cutler A. Claire, Haufler Virginia, Porter Tony (dir.), *Private Authority and International Affairs*, Albany, Suny Press, 1999.

[37] Brunson Nils, Jacobson Bengt (dir.), *A World of Standards*, Oxford, Oxford University Press, 2000, p. 1.

3.2. La norme comme « dispositif cognitif collectif »

Au-delà de sa fonction technique d'interopérabilité, la norme remplit une fonction cognitive essentielle. L'économiste Olivier Favereau a ainsi proposé de la concevoir comme un *« dispositif cognitif collectif »*[38] : elle fournit aux acteurs un cadre commun d'interprétation du monde, qui leur permet de coordonner leurs anticipations et leurs actions. La taxonomie proposée par Paul David distingue ainsi plusieurs types de normes selon leur fonction[39] :

- Les normes dites de base ou fondamentales. Ces normes concernent les référentiels de terminologie, de poids et mesure ou encore de dimension. Elles permettent de fixer un vocabulaire commun et sont souvent des fondations essentielles à d'autres normes plus techniques. En effet, les normes de base relèvent plus de connaissances scientifiques que du savoir-faire technique.

- Les normes de qualité ou d'organisation. Ces normes sont là pour décrire les mécanismes de fonctionnement d'une entité, ou encore un seuil minimum de qualité, de sécurité ou de performance à atteindre.
- Les normes d'interopérabilité ou de compatibilité, quant à elles, définissent les conditions techniques à respecter pour rendre interopérables des produits ou systèmes.

Peut être également cité ici George Akerlof, qui, dans son célèbre article sur le « *marché des citrons »*[40], avait montré comment l'asymétrie d'information peut conduire à l'effondrement des marchés. Autrement dit, si les acheteurs ne peuvent distinguer les bons produits des mauvais, ils ne sont pas prêts à payer le prix des bons produits, ce qui conduit les vendeurs de bons produits à quitter le marché. Les normes de qualité constituent une réponse à ce problème. En certifiant que les produits répondent à certaines spécifications, elles restaurent la confiance et permettent aux marchés de fonctionner.

Cette fonction cognitive de la norme a des implications géopolitiques importantes. La norme ne se contente pas de résoudre des problèmes techniques, elle façonne les catégories de pensée à travers lesquelles les acteurs appréhendent le monde. En définissant ce qui est « normal », « standard »,

---

38 Favereau Olivier, « Marchés internes, marchés externes », *Revue économique*, vol. 40, n° 2, 1989, pp. 273-328.

39 David Paul A., « Some New Standards for the Economics of Standardization in the Information Age », in DASGUPTA Partha, Stoneman Paul (dir.), *Economic Policy and Technological Performance*, Cambridge, Cambridge University Press, 1987, pp. 206-239

40 Akerlof George A., « The Market for 'Lemons': Quality Uncertainty and the Market Mechanism », *The Quarterly Journal of Economics*, vol. 84, n° 3, 1970, pp. 488-500.

« conforme », et par conséquent attendu. Elle contribue également à populariser certaines configurations technologiques et à en marginaliser d'autres. Contrôler la définition des normes, c'est ainsi exercer une forme de pouvoir sur la manière dont les acteurs pensent et agissent.

3.3. Effets de réseau, rendements croissants et dépendance normative

L'économie de la normalisation est caractérisée par des phénomènes de rendements croissants et d'effets de réseau. Ainsi, W. Brian Arthur a montré que dans certains domaines technologiques, l'adoption d'une technologie par un acteur augmente l'incitation des autres acteurs à l'adopter également[41]. Plus une norme est adoptée, plus il devient coûteux de s'en écarter, et plus elle devient attractive pour les nouveaux entrants. Ce mécanisme conduit à des phénomènes de *lock-in* (littéralement en anglais : enfermement), une fois qu'une norme s'est imposée, il devient très difficile de la remplacer, même si des alternatives techniquement supérieures existent.

L'exemple classique est celui du clavier QWERTY, analysé par Paul David[42]. Cette disposition des touches, héritée des contraintes mécaniques des machines à écrire du XIXe siècle, s'est imposée comme standard mondial malgré l'existence d'alternatives ergonomiquement plus efficaces (comme le clavier Dvorak). Une fois que des millions de personnes ont appris à taper sur un clavier QWERTY, le coût de basculement vers un autre standard devient prohibitif.

Ces phénomènes de dépendance normative ont des implications géopolitiques majeures. Ils suggèrent que les choix normatifs effectués à un moment donné peuvent avoir des conséquences durables, voire irréversibles. Être présent dès les premières phases de l'élaboration d'une norme confère donc un avantage stratégique considérable. Il est beaucoup plus facile d'influencer une norme en cours d'élaboration que de modifier une norme déjà établie. Cette dynamique explique l'intensité des rivalités dans les comités de normalisation et l'importance pour les États de maintenir une présence active dans ces arènes[43].

---

41 Arthur W. Brian, « Competing Technologies, Increasing Returns, and Lock-In by Historical Events », *The Economic Journal*, vol. 99, n° 394, 1989, pp. 116-131.

42 David Paul A., « Clio and the Economics of QWERTY », *The American Economic Review*, vol. 75, n° 2, 1985, pp. 332-337.

43 Hawkins Richard, Mansell Robin, SKEA Jim (dir.), *Standards, Innovation and Competitiveness: The Politics and Economics of Standards in Natural and Technical Environments*, Cheltenham, Edward Elgar, 1995.

3.4. Les « batailles de standards » et leurs enjeux géopolitiques

Schmidt et Werle, dans leur étude sur la normalisation des télécommunications, ont montré que l'élaboration des normes ne répond pas seulement à une logique de rationalité technique, mais est également traversée par des rapports de force entre acteurs[44]. Les « batailles de standards » (*standards wars*) opposent des coalitions d'acteurs qui cherchent à faire prévaloir leurs solutions technologiques, chacune étant associée à des intérêts économiques et parfois géopolitiques distincts[45].

Mattli et Büthe ont également identifié plusieurs facteurs qui expliquent la capacité d'un acteur à faire prévaloir ses positions dans les processus de normalisation[46]. Il y a en premier lieu les ressources financières (la participation aux comités techniques a un coût), mais également l'expertise technique (il faut pouvoir argumenter sur le fond), les réseaux relationnels (le consensus se construit dans les couloirs autant que dans les réunions formelles), et la cohérence institutionnelle (un acteur qui parle d'une seule voix pèse plus qu'un acteur fragmenté). Ces facteurs créent des asymétries structurelles entre acteurs[47]. Ainsi, les grandes entreprises et les grands États disposent d'avantages comparatifs en matière d'investissement financier et humain que les petits acteurs peinent à compenser.

Anu Bradford, dans *The Brussels Effect*, a par exemple, montré comment l'Union européenne est parvenue à imposer ses standards réglementaires à l'échelle mondiale, non pas par la coercition, mais par la seule force de l'importance de son marché intérieur[48]. Les entreprises qui veulent accéder au marché européen doivent se conformer aux normes européennes, et une fois qu'elles ont adapté leurs produits à ces normes, elles tendent à les appliquer également sur d'autres marchés pour des raisons d'économies d'échelle. Ce mécanisme d'« effet Bruxelles » illustre comment la normalisation peut devenir un instrument de projection de puissance, même en l'absence de domination militaire ou économique directe.

---

[44] Schmidt Susanne K., Werle Raymund, *Coordinating Technology: Studies in the International Standardization of Telecommunications*, Cambridge (MA), MIT Press, 1998, p. 15

[45] Simcoe Timothy, « Standard Setting Committees: Consensus Governance for Shared Technology Platforms », *American Economic Review*, vol. 102, n° 1, 2012, pp. 305-336.

[46] Mattli Walter, Büthe Tim, « Setting International Standards: Technological Rationality or Primacy of Power? », *World Politics*, vol. 56, n° 1, 2003, pp. 1-42.

[47] Farrel Joseph, SALONER Garth, « Coordination Through Committees and Markets », *The RAND Journal of Economics*, vol. 19, n° 2, 1988, pp. 235-252.

[48] Bradford Anu, « The Brussels Effect: How the European Union Rules the World », *Oxford, Oxford University Press, 2020, p.2.*

3.5. « Code is law » : les normes techniques comme instruments de pouvoir

Dans le domaine spécifique du cyberespace, plusieurs auteurs ont souligné la dimension politique des normes techniques. Lawrence Lessig, dans sa formule désormais célèbre « Code is law », a montré que le code informatique, c'est-à-dire l'ensemble des protocoles, standards et logiciels qui structurent l'espace numérique, exerce une fonction de régulation analogue à celle du droit[49]. Comme le droit, le code définit ce qui est possible et ce qui ne l'est pas, ce qui est autorisé et ce qui est interdit. Mais contrairement au droit, qui est le produit de délibérations politiques explicites, le code est souvent présenté comme un artefact purement technique, soustrait au débat démocratique.

Laura DeNardis, dans ses travaux sur la gouvernance d'Internet, a prolongé cette analyse en montrant comment les « protocoles techniques » constituent des *« instruments de pouvoir »*[50]. Les choix effectués dans la conception des protocoles de communication, quelles informations sont collectées, comment elles sont transmises, qui peut y accéder, ont des implications directes sur la vie privée, la liberté d'expression, la sécurité nationale. Milton Mueller, dans *Networks and States*, a analysé les conflits géopolitiques autour de la gouvernance d'Internet, montrant comment les États cherchent à reprendre le contrôle sur des infrastructures initialement conçues selon une logique décentralisée et transnationale[51].

Langdon Winner avait posé dès 1980 la question fondamentale : *« Les artefacts techniques ont-ils une politique ? »*[52] Sa réponse était positive. Autrement dit, les choix de conception technique ne sont jamais neutres, mais incorporent des valeurs et des rapports de pouvoir. Cette perspective a été développée par les travaux de Susan Leigh Star sur les infrastructures et par Geoffrey Bowker et Susan Leigh Star sur les systèmes de classification. Ces travaux montrent que les standards techniques, loin d'être de simples outils neutres, sont des constructions sociales qui véhiculent des représentations du monde et des intérêts particuliers[53] [54].

---

[49]Lessig Lawrence, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999, p. 6 : « Code is law ».

[50]Denardis Laura, *Protocol Politics: The Globalization of Internet Governance*, Cambridge (MA), MIT Press, 2009, p. 6.

[51]Mueller Milton, *Networks and States: The Global Politics of Internet Governance*, Cambridge (MA), MIT Press, 2010, p. 5.

[52]Winner Langdon, « Do Artifacts Have Politics? », *Daedalus*, vol. 109, n° 1, 1980, pp. 121-136.

[53]Star Susan Leigh, « The Ethnography of Infrastructure », *American Behavioral Scientist*, vol. 43, n° 3, 1999, pp. 377-391.

[54]Bowker Geoffrey C., STAR Susan Leigh, *Sorting Things Out: Classification and Its Consequences*, Cambridge (MA), MIT Press, 1999.

4. La spécificité des données géographiques numériques

4.1. La carte comme instrument de pouvoir : apports de la cartographie critique

L'analyse géopolitique de la normalisation des données géographiques numériques peut s'appuyer sur les apports de la cartographie critique. Depuis les travaux pionniers de John Brian Harley sur la « déconstruction de la carte »[55], un courant de recherche s'est développé autour de l'idée que les cartes ne sont pas des représentations neutres et objectives du monde, mais des constructions sociales qui véhiculent des visions du monde et des intérêts particuliers. Denis Wood et John Fels ont montré comment les cartes constituent des « instruments de pouvoir » utilisés par les États pour affirmer leur contrôle sur les territoires[56] . De même, le professeur Philippe Boulanger a souligné le rôle historique de la cartographie militaire dans l'exercice de la puissance étatique[57].

La numérisation de la cartographie n'a pas mis fin à ces enjeux de pouvoir, bien au contraire, elle les a transformés et complexifiés. L'émergence de ce que Michael Goodchild a appelé la « volunteered geographic information »[58], l'information géographique produite par les citoyens via leurs smartphones et les plateformes participatives, a bouleversé le monopole traditionnel des États et des instituts géographiques nationaux sur la production cartographique. Sarah Elwood et Agnieszka Leszczynski ont ainsi analysé les « nouvelles politiques du savoir »[59] qui émergent de cette démocratisation de la production de données géographiques.

[55]Harley John Brian, « Deconstructing the Map », *Cartographica*, vol. 26, n° 2, 1989, pp. 1-20.

[56]Wood Denis, FELS John, *The Power of Maps*, New York, Guilford Press, 1992.

[57]Boulanger Philippe, *La géographie, reine des batailles*, Paris, Perrin, 2020, p. 45.

[58]Goodchild Michael F., « Citizens as sensors: the world of volunteered geography », *GeoJournal*, vol. 69, n° 4, 2007, pp. 211-221.

[59] Elwood, Sarah et Leszczynski, Agnieszka. « New spatial media, new knowledge politics », *Transactions of the Institute of British Geographers*, vol. 38, n° 4, 2013, p. 544-559.

4.2. La dualité ontologique des données géographiques numériques

Comme établi précédemment, les données géographiques numériques occupent donc une position singulière dans l'architecture du cyberespace. Elles sont à la fois un objet du cyberespace et une représentation de l'espace physique. Cette dualité ontologique a plusieurs implications pour l'analyse conduite dans cette thèse.

En premier lieu, elle confère aux données géographiques une dimension stratégique renforcée. Contrairement à d'autres types de données numériques, les données géographiques touchent directement à la connaissance et à la représentation du territoire, des prérogatives régaliennes par excellence. La maîtrise de ces données engage la capacité d'un État à connaître son propre territoire, à le défendre, à y projeter sa puissance. C'est pourquoi les données géographiques ont historiquement fait l'objet d'un contrôle étatique étroit, et pourquoi leur normalisation soulève des enjeux de souveraineté spécifiques.

D'autre part, la dualité ontologique fait des données géographiques un vecteur de l'interpénétration entre cyberespace et espace physique. À travers les systèmes de navigation par satellite, les cartes numériques embarquées, ou encore les applications de géolocalisation, les données géographiques irriguent désormais l'ensemble des activités humaines, qu'elles soient civiles ou militaires. Les normes qui régissent ces données ne concernent donc pas seulement le cyberespace, elles affectent directement les conditions de l'action dans l'espace physique.

Enfin, la dualité ontologique expose les données géographiques à des menaces spécifiques. Une cyberattaque visant des données géographiques peut avoir des conséquences dans l'espace physique : brouillage GPS affectant la navigation aérienne ou maritime, manipulation de cartes numériques conduisant à des erreurs de positionnement, compromission de systèmes d'information géographique militaires. Ces menaces justifient une attention particulière aux enjeux de sécurité dans la normalisation des données géographiques.

5. Démarche méthodologique

Le cadre théorique ayant été posé, il convient à présent d'expliciter la démarche méthodologique qui a présidé à l'enquête de terrain. L'analyse géopolitique de la normalisation des données géographiques numériques nécessite en effet une méthodologie adaptée à cet objet d'étude, situé à l'intersection de plusieurs champs disciplinaires et de plusieurs échelles spatiales. La normalisation, processus éminemment technique en apparence, se révèle être traversée par des logiques de pouvoir, des stratégies d'acteurs et des représentations qu'il s'agit de mettre au jour. Cette réalité a nécessité la mise en place de plusieurs méthodes d'enquêtes. En premier lieu, l'entretien semi-directif, pour accéder aux discours et aux représentations des acteurs, puis l'observation participante, pour saisir les dynamiques d'interaction au sein des arènes de normalisation, mais également l'analyse documentaire, pour replacer ces observations dans leur contexte institutionnel et historique. L'enquête empirique s'est déployée sur une période de deux ans, de mars 2022 à décembre 2023, au cours de laquelle vingt-cinq entretiens ont été conduits et plus de cent dix réunions observées, à toutes les échelles de la gouvernance normative.

5.1. Positionnement épistémologique et approche multiscalaire

Cette recherche s'inscrit dans une perspective d’analyse, héritière de la tradition weberienne des sciences sociales. L'objectif ici n'est pas seulement de décrire les mécanismes de la normalisation des données géographiques numériques, mais de comprendre le sens que les acteurs confèrent à leurs pratiques, les stratégies qu'ils déploient dans les arènes normatives et les représentations qui orientent leurs choix. Accorder une importance particulière aux discours des acteurs, à leurs justifications, à leurs perceptions des enjeux et des rapports de force apparaît ici comme capital afin de pouvoir comprendre les enjeux géopolitiques de la normalisation des données géographiques. Cette approche implique également une attention soutenue aux dimensions symboliques et cognitives de la normalisation, conformément à la conception de la norme comme *« dispositif cognitif collectif »* développée par Olivier Favereau évoquée plus haut.

Cette approche se veut également multiscalaire. Les processus de normalisation des données géographiques se déploient en effet à plusieurs échelles emboîtées qui interagissent constamment : l'échelle internationale, où s'élaborent les normes au sein de l'ISO/TC 211, de l'OGC ou du DGIWG, l'échelle européenne, structurée par le CEN, la directive INSPIRE et les travaux d'EuroGeographics,

l'échelle nationale, articulée autour de l'AFNOR, du CNIG et de l'IGN, enfin, l'échelle territoriale, où les DREAL, les CRIGEs et les plateformes régionales traduisent, adaptent et parfois contestent les standards élaborés aux échelons supérieurs. L'articulation de ces différentes échelles constitue un enjeu analytique central de cette thèse. Les décisions prises dans les arènes internationales se répercutent sur les pratiques locales, tandis que les remontées de terrain peuvent influencer, parfois, les orientations nationales. Cette circulation multiscalaire des normes et des pratiques impose une méthodologie capable de saisir ces interactions et ces effets de rétroaction.

Enfin, ce travail de recherche mobilise une approche pluridisciplinaire, à l'image de la normalisation elle-même. La normalisation des données géographiques numériques se situe en effet à l'intersection de la géopolitique, de la géographie, des sciences de l'information, de l'économie politique et du droit. Cette pluridisciplinarité se traduit par le recours à des sources et des cadres d'analyse variés, tels que les travaux de Frédérick Douzet et Amaël Cattaruzza sur la géopolitique du cyberespace voisinent avec ceux de Tim Büthe et Walter Mattli sur l'économie politique de la normalisation.

5.2. Le corpus d'entretiens : diversité des acteurs et des échelles

Le matériau empirique principal de cette recherche repose sur une série de vingt-cinq entretiens semi-directifs conduits entre mars 2022 et juin 2023. Le choix de l'entretien semi-directif se justifie par la nature exploratoire de cette recherche sur un objet encore peu étudié dans la littérature géopolitique francophone. Cette méthode permet de saisir les représentations et les stratégies des acteurs dans leur complexité, tout en laissant émerger des thématiques non anticipées par le chercheur. Elle s'avère particulièrement adaptée à l'étude d'un milieu professionnel spécialisé, où les enjeux techniques et les enjeux politiques s'entremêlent étroitement.

La constitution du corpus a obéi à plusieurs critères. Le premier tient à la position institutionnelle des enquêtés. Il s'agissait ici de rencontrer des acteurs disposant d'une connaissance approfondie des enjeux de la normalisation ou de la gestion des données géographiques à leur échelle d'intervention. Le deuxième critère concerne la diversité des profils, le corpus rassemble des experts de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), des officiers géographes du ministère des Armées, des responsables de l'Institut national de l'information géographique et forestière (IGN) et du Conseil national de l'information géolocalisée (CNIG), des directeurs de plateformes régionales et de centres régionaux d'information géographique (CRIGEs), des pilotes des systèmes

d'information des directions régionales de l'environnement, de l'aménagement et du logement (DREAL), des acteurs du secteur privé ainsi que des chercheurs spécialisés. Le troisième critère porte sur la répartition géographique, les entretiens couvrent plusieurs régions métropolitaines (Normandie, Bretagne, Corse, Hauts-de-France, Auvergne-Rhône-Alpes) et ultramarines (Martinique), ainsi que des terrains internationaux (Stockholm, Garmisch-Partenkirchen, Jeonju).

Tableau 1 : Corpus d'entretiens semi-directifs

Institution	Personne(s)	Fonction / Contexte	Date
ANSSI	Anonymisé pour la version de diffusion	Expert cybersécurité	02/03/2022
ANSSI	Anonymisé pour la version de diffusion	Expert cybersécurité	10/03/2022
BGHOM (Armées)	Anonymisé pour la version de diffusion	Officier géographe	14/03/2022
BGHOM (Armées)	Anonymisé pour la version de diffusion	Chef de bureau BGHOM	14/03/2022
IGN	Anonymisé pour la version de diffusion	Chargé relations européennes et internationales	15/03/2022
IGN	Anonymisé pour la version de diffusion	Chef de service adjoint partenariats	15/03/2022
IGN	Anonymisé pour la version de diffusion	Expert normalisation	17/03/2022
Géo212 (privé)	Anonymisé pour la version de diffusion	Directeur	23/03/2022
CNIG	Anonymisé pour la version de diffusion	Directeur général	07/05/2022
IGN	Anonymisé pour la version de diffusion	Expert normalisation ISO	27/09/2022
28e Groupe Géographique	Anonymisé pour la version de diffusion	Officier géographe	28/11/2022
OpenIG	Anonymisé pour la version de diffusion	Responsables SI	03/02/2023

DREAL Corse	Anonymisé pour la version de diffusion	Chef unité données	03/02/2023
DREAL Corse	Anonymisé pour la version de diffusion	Resp. informatique	06/02/2023
DREAL Normandie	Anonymisé pour la version de diffusion	Équipe SI	13/02/2023
DEAL Martinique	Anonymisé pour la version de diffusion	Resp. géomatique	14/02/2023
DREAL Hauts-de-France	Anonymisé pour la version de diffusion	Resp. SI observation	16/02/2023
DREAL Bretagne	Anonymisé pour la version de diffusion	Pilote SI	20/02/2023
CRAIG	Anonymisé pour la version de diffusion	Resp. informatique	23/02/2023
DGA	Anonymisé pour la version de diffusion	Expert défense	13/03/2023
Collectivité de Corse	Anonymisé pour la version de diffusion	Responsables données	16/03/2023
Région Normandie / CRIGE	Anonymisé pour la version de diffusion	Équipe CRIGE	22/03/2023
GEOCAPI (Armées)	Anonymisé pour la version de diffusion	Directeur	28/03/2023
CNIG	Anonymisé pour la version de diffusion	Animateur Europe, DG	15/06/2023
IGN	Anonymisé pour la version de diffusion	Resp. de département Normalisation et référentiels	20/06/2023

Source : Enquête de terrain, 2022-2023.

La répartition institutionnelle du corpus se devait également de refléter la structure de l'écosystème français de la normalisation géospatiale. Les acteurs étatiques civils (IGN, CNIG, ANSSI, DREAL, DEAL) représentent six entretiens sur dix, ce qui reflète le rôle central de l'État dans la production et la régulation des données géographiques en France. Les acteurs de la défense (Bureau Géographie, Hydrographie, Océanographie et Météorologie, 28e Groupe Géographique, GEOCAPI, Direction générale de l'armement) constituent un second ensemble, indispensable pour appréhender les enjeux spécifiques de la normalisation militaire. Les acteurs territoriaux (CRIGEs, plateformes régionales, collectivités) permettent de saisir les dynamiques infra-nationales et les tensions entre centralisation et autonomie locale. Enfin, les chercheurs spécialisés et les acteurs internationaux (Open Geospatial Consortium) apportent des perspectives comparatives et analytiques précieuses.

Tableau 2 : Répartition institutionnelle des entretiens

Catégorie d'acteurs	**Nombre**	**Proportion**
État civil (IGN, CNIG, ANSSI)	9	36 %
Services déconcentrés (DREAL, DEAL)	6	24 %
Défense (BGHOM, 28e GG, GEOCAPI, DGA)	5	20 %
Acteurs territoriaux (CRIGEs, collectivités)	4	16 %
Secteur privé (Géo212)	1	4 %
Total	**25**	**100 %**

Source : Enquête de terrain, 2022-2023.

Les entretiens ont été conduits à partir d'une grille semi-directive organisée autour de cinq axes thématiques, adaptée en fonction du profil de chaque enquêté. Le premier axe portait sur le parcours professionnel de l'enquêté et son rôle au sein de l'institution, afin de contextualiser son discours et de comprendre sa position dans le champ de l'information géographique. Le deuxième axe concernait les pratiques concrètes de production et de gestion des données géographiques, qu’il s’agisse des formats utilisés, normes suivies, difficultés rencontrées, arbitrages effectués. Le troisième axe explorait les relations avec les autres acteurs de l'écosystème (État, collectivités, plateformes régionales, IGN, CNIG, organisations internationales), les modalités de coopération et les éventuelles tensions. Le quatrième axe abordait les enjeux de cybersécurité et de protection des données. À la fois la perception

des menaces, les mesures mises en œuvre, et les incidents éventuels. Le cinquième axe, enfin, invitait les enquêtes à exprimer leurs représentations de la souveraineté numérique et des enjeux géopolitiques de la normalisation, ainsi que leurs anticipations quant aux évolutions futures.

Les entretiens, d'une durée moyenne d'une heure à deux heures, ont été enregistrés lorsque l'accord des personnes interrogées a pu être obtenu, puis retranscrits. Les citations mobilisées dans le corps de la thèse ont fait l'objet, lorsque cela était requis, d'une validation par les enquêtés, notamment pour les acteurs relevant du ministère des Armées.

5.3. L'observation participante : une immersion dans les arènes de normalisation

L'enquête de terrain a été complétée par une démarche d'observation participante au sein des instances nationales et internationales de normalisation. Cette méthode, classique en anthropologie et en sociologie des organisations, permet d'accéder à des données inaccessibles par l'entretien ou l'analyse documentaire seuls, notamment les interactions informelles entre délégations, les rapports de force non explicités dans les comptes rendus officiels, les stratégies de négociation, ainsi que les rituels institutionnels qui scandent la vie des comités techniques. L'observation participante s’est avérée particulièrement utile pour l'étude des processus de normalisation, où le consensus affiché masque souvent des tensions et des arbitrages dont la trace écrite reste rares. Au total, plus de cent dix réunions ont été observées sur la période 2022-2023, à différentes échelles de la gouvernance normative.

À l'échelle nationale, l'observation des travaux du Conseil national de l'information géolocalisée (CNIG) a constitué un axe majeur de l'enquête. Les réunions de la Commission des Standards, de la Commission Règles et Qualité, de la Commission Modèles Économiques ainsi que les Conseils pléniers ont été suivis de manière régulière entre mai 2022 et décembre 2023. Les groupes de travail thématiques (Risques, Droit des sols et urbanisme, Bâti, Occupation du sol à grande échelle, Métadonnées, Dinamis) ont fait l'objet d'une observation systématique, offrant un accès privilégié aux débats techniques et aux négociations qui précèdent la publication des standards. Ces observations ont permis de saisir les dynamiques de coopération et de conflit entre les différents acteurs représentés au sein du CNIG, qu’il s’agisse des ministères, des établissements publics, des collectivités territoriales, ou encore des entreprises privées. Elles ont également mis en lumière le rôle des individus dans la fabrique des normes, au-delà des positions institutionnelles.

L'accès aux réunions des programmes de coproduction internationaux militaire a constitué un apport décisif pour l'accomplissement de ce travail de recherche. Le programme MGCP (Multinational Geospatial Co-production Program), qui rassemble les agences géographiques militaires de plusieurs pays pour la production de données vecteurs au 50 000e, a été observé lors de ses réunions plénières (Strasbourg, avril 2023) et de ses groupes techniques (Future Strategy Technical Subgroup). Le programme TREx (TanDEM-X High Resolution Elevation Data Exchange), dédié à l'élaboration de modèles numériques de terrain de haute résolution, le programme MUVD (Multinational Urban Vector Data), consacré aux données vecteurs urbaines, et le programme IPHG (International Programme for Human Geography), qui vise à standardiser les données de géographie humaine, ont également fait l'objet d'une observation régulière. Ces programmes, d'accès restreint, constituent des lieux privilégiés d'élaboration des spécifications techniques qui serviront de base aux futurs standards de défense. Il est à noter que leur observation a permis de documenter des dynamiques encore jamais étudiés dans la littérature académique.

À l'échelle internationale, la participation aux travaux de l'ISO/TC 211 (Information géographique/Géomatique) a constitué un volet essentiel de l'enquête. La 55e réunion plénière de Stockholm (décembre 2022) et la 56e réunion plénière de Jeonju, en Corée du Sud (mai 2023), ont permis d'observer les dynamiques géopolitiques à l'œuvre dans la normalisation internationale. Qu'il s'agisse de l'affirmation des stratégies nationales, de la formation d'alliances entre délégations, de la montée en puissance des acteurs asiatiques, ou encore, de l'articulation parfois tendue entre les consortiums privés tels que l'Open Geospatial Consortium et l'ISO. Les groupes de travail (WG1 sur les cadres de référence, WG6 sur l'imagerie, WG7 sur les communautés d'information, WG9 sur la qualité des données, et le WG10 sur l'accès universel) et les groupes consultatifs (AG1 Outreach, AG2 Strategy, Joint Advisory Group avec l'OGC) ont été suivis de manière régulière, y compris par visioconférence entre les sessions plénières. Les séminaires « Standards in Action » ont permis de saisir les enjeux de la diffusion et de l'appropriation des normes par les utilisateurs finaux.

Le Defence Geospatial Information Working Group (DGIWG) a fait l'objet d'une observation approfondie. Ce groupe multinational, qui rassemble vingt-quatre nations liées par un protocole d'accord pour l'élaboration de standards géospatiaux de défense, constitue une arène cruciale pour la compréhension des enjeux militaires de la normalisation. Les réunions du Panel 5 (Web Services Technical Panel), chargé de développer les standards relatifs aux services web géospatiaux, ont été observées à Munich (mars 2023) et à Pont-à-Mousson (avril 2023), ainsi que via plusieurs réunions en visioconférence sur la même période. La réunion plénière de Garmisch-Partenkirchen, en Allemagne (octobre 2023), a permis de saisir l'articulation entre les travaux des différents panels et les orientations

stratégiques du groupe. Les échanges informels avec les délégués d'autres pays ont fourni des éclairages précieux sur les stratégies nationales et sur la perception des mutations géopolitiques en cours, notamment la montée en puissance de la Chine dans les instances de normalisation civile.

Tableau 3 : Synthèse des observations participantes par niveau scalaire

Échelle	**Instances observées**	**Nb réunions**	**Période**
Nationale	CNIG (commissions, groupes de travail, pôles, conseil plénier)	33	2022-2023
Défense / OTAN	MGCP, TREx, MUVD, IPHG (plénières, groupes techniques)	28	2022-2023
Internationale civile	ISO/TC 211 (groupes de travail, groupes consultatifs, plénières)	35	2022-2023
Internationale défense	DGIWG (panels techniques, plénières), SIFWG	20	2023
Total		**116**	

Source : Enquête de terrain, 2022-2023.

L'accès à ces terrains d'observation a été rendu possible par une insertion progressive dans les réseaux professionnels de la normalisation géospatiale, notamment par une participation active aux travaux du CNIG et de l'ISO/TC 211 en tant que membre de la délégation française. L’accès à cette position a été un élément crucial dans l’accomplissement de ce travail de thèse et l’auteur de cette thèse ne saurait assez remercier les personnes qui ont rendu cela possible. Elle a facilité l'accès à des arènes fermées, permis une compréhension fine des enjeux techniques qui sous-tendent les débats apparemment procéduraux, et conféré à l’auteur une légitimité auprès des acteurs enquêtés.

5.4. Le corpus documentaire : normes, stratégies et littérature grise

L'analyse documentaire constitue le troisième pilier de la démarche méthodologique. Le corpus mobilisé ici peut être structuré en quatre ensembles distincts. Le premier rassemble les normes et standards techniques qui constituent le cœur de l'objet d'étude. La série ISO 19100, qui forme l'architecture de référence pour l'information géographique (ISO 19115 sur les métadonnées, ISO 19157 sur la qualité, ISO 19131 sur les spécifications de produits, ISO 19139 sur l'implémentation des métadonnées en XML, entre autres), a fait l'objet d'une analyse approfondie. Les standards de l'Open Geospatial Consortium (Web Map Service, Web Feature Service, GeoPackage, API Features, SensorThings) ont été étudiés tant dans leur contenu technique que dans leur processus d'élaboration. Les accords de normalisation de l'OTAN (STANAG) pertinents pour l'information géographique, les spécifications du DGIWG (Defence Geospatial Information Framework, Defence Feature Data Dictionary, profils d'implémentation) ainsi que les standards nationaux publiés par le CNIG complètent ce premier ensemble. L'analyse de ces documents a porté sur leur contenu prescriptif, mais aussi sur leurs silences et leurs ambiguïtés, qui révèlent souvent les compromis passés entre parties prenantes.

Le deuxième ensemble comprend les documents institutionnels et stratégiques qui encadrent les processus de normalisation. Parmi les sources françaises figurent les rapports parlementaires (le rapport Faure-Muntian sur les données géographiques souveraines, le rapport Capo-Canellas sur l'IGN), les textes réglementaires (décrets relatifs au CNIG et au système français de normalisation), les documents stratégiques de l'IGN (contrat d'objectifs et de performance, stratégie 2021-2025) et les publications de l'ANSSI relatives à la cybersécurité. À l'échelle européenne, la directive INSPIRE et ses documents d'accompagnement, le Data Governance Act, le Data Act ainsi que les communications de la Commission européenne sur la stratégie normative ont été mobilisés. Les documents des organisations internationales de normalisation (directives ISO/IEC, rapports annuels, études prospectives) complètent ce corpus institutionnel.

Le troisième ensemble est constitué de la littérature grise, souvent difficile d'accès, mais riche en informations sur les débats internes aux communautés de normalisation. Les comptes rendus de réunions du CNIG, de l'ISO/TC 211, du DGIWG et des programmes de coproduction fournissent une trace des discussions et des arbitrages qui précèdent la publication des normes. Les présentations techniques diffusées lors des événements professionnels (séminaires Standards in Action, conférences de l'AFIGéo, journées EuroGeographics) permettent de saisir les enjeux de l'appropriation des normes par les utilisateurs. Les études sectorielles (rapports de l'AFIGéo sur les plateformes territoriales, études

KPMG sur le cloud européen, travaux de l'Egis Conseil sur les jumeaux numériques) et les publications de think tanks (IFRI, Asia Society Policy Institute) apportent des éclairages complémentaires sur les dimensions économiques et géopolitiques de la normalisation.

Le quatrième ensemble rassemble la littérature académique mobilisée pour construire le cadre théorique et interpréter les données empiriques. Les travaux en géopolitique du cyberespace (Frédérick Douzet, Amaël Cattaruzza, Kevin Limonier, Stéphane Taillat), en économie politique de la normalisation (Tim Büthe, Walter Mattli, Jean-Christophe Graz, Anu Bradford), en gouvernance des données (Laura DeNardis, Milton Mueller) et en études de normalisation (Nils Brunsson, Bengt Jacobsson) constituent les principales références théoriques de cette recherche.

Conclusion de la section théorique

Ainsi, cette section a posé les fondements théoriques de cette thèse, en articulant trois perspectives complémentaires. La géopolitique du cyberespace, la conceptualisation de la souveraineté numérique, et l'économie politique de la normalisation. En premier lieu, il apparaît que la normalisation des données géographiques numériques peut être analysée comme un objet géopolitique à part entière, traversé par des rivalités de pouvoir entre acteurs aux intérêts divergents. Une définition de la souveraineté numérique qui met l'accent sur la dimension normative a été exposée. Ainsi, est souverain celui qui peut participer de manière significative à la définition des règles qui structurent l'espace numérique. Enfin, les apports de l'économie politique de la normalisation ont permis de souligner les dynamiques de pouvoir à l'œuvre dans ces processus. Ce cadre théorique oriente la démarche empirique de ce travail. Il invite à analyser les processus de normalisation non pas comme des exercices de rationalité technique détachés des enjeux de pouvoir, mais comme des arènes où se négocient des rapports de force, où se jouent des intérêts économiques et stratégiques, où se projettent des visions du monde. Il conduit à porter une attention particulière aux asymétries entre acteurs, aux mécanismes de verrouillage et de dépendance, aux articulations entre échelles nationale, européenne et internationale. Enfin, il permet de comprendre pourquoi les États, et en particulier la France, ont un intérêt stratégique à participer activement aux processus de normalisation des données géographiques numériques. Il ne s'agit pas ici seulement de faciliter l'interopérabilité technique, mais de défendre une certaine conception de la souveraineté à l'ère numérique.

Ce cadre conceptuel ainsi posé, il convient désormais de le confronter à la réalité empirique de la normalisation des données géographiques. Les trois parties qui structurent cette thèse procèdent selon une logique d'approfondissement progressif. La première partie s'attache à comprendre les fondements historiques, institutionnels et géopolitiques de la normalisation géospatiale. Elle aborde en premier lieu comment cet écosystème s'est constitué, quels acteurs y interviennent, et quels rapports de force le traversent. La deuxième partie analyse les vulnérabilités de cet écosystème face au risque cyber, en montrant comment les normes peuvent constituer à la fois des vecteurs de fragilité et des instruments de résilience. La troisième partie, enfin, se projette dans l'avenir pour interroger les stratégies que la France peut déployer afin de préserver sa souveraineté dans un contexte de fragmentation normative mondiale. Cette progression a été choisi, afin de permettre au lecteur de saisir les enjeux de souveraineté à différentes échelles temporelles et spatiales.

Partie 1 : Comprendre la normalisation des informations géographiques numériques

Le cadre théorique a établi que la normalisation des données géographiques numériques constitue un espace normatif au sens géopolitique du terme. Il s'agit d'un territoire immatériel approprié par des acteurs aux intérêts divergents, traversé par des rivalités de pouvoir, et dont le contrôle engage la souveraineté des États. Cette première partie vise à donner corps à cette proposition théorique en examinant empiriquement l'écosystème de la normalisation géospatiale. Trois chapitres structurent cette analyse.

Le Chapitre I pose les fondements en retraçant l'histoire de la normalisation et en montrant comment la France s'est inscrite dans cet environnement. Il explicite également les spécificités des données géographiques numériques en matière de normalisation et de cybersécurité, prolongeant ainsi l'analyse de leur dualité ontologique esquissée dans le cadre théorique. Le Chapitre II cartographie l'écosystème institutionnel de la normalisation géospatiale, à l'échelle internationale (ISO, OGC), européenne (CEN, INSPIRE) et militaire (DGIWG, OTAN) Il vise à mettre en lumière les interdépendances et les tensions entre ces différents niveaux de gouvernance. Le Chapitre III, enfin, analyse les enjeux propres aux différentes catégories d'acteurs, qu'il s'agisse des États, des entreprises, ou encore des armées, en montrant comment chacun mobilise la normalisation comme instrument de pouvoir, selon la logique des batailles de standards identifiée par Schmidt et Werle. À l'issue de cette première partie, le lecteur disposera d'une cartographie complète de l'écosystème normatif géospatial et des rapports de force qui le structurent, préalable indispensable à l'analyse des vulnérabilités cyber qui seront plus amplement étudiées de la deuxième partie.

Chapitre I - Géopolitique et normalisation des données géographiques

Le cadre théorique a montré que la norme ne se réduit pas à sa fonction technique d'interopérabilité, elle constitue également un dispositif cognitif collectif qui façonne les représentations et structure les rapports de pouvoir entre acteurs. Avant d'analyser comment cette dimension politique se déploie concrètement dans le domaine des données géographiques, il convient de revenir sur la définition institutionnelle de la norme et sur l'histoire de son institutionnalisation.

L'Organisation internationale de standardisation (ISO)[60] définie la norme comme étant, *« l'activité consistant à établir, au regard de problèmes réels ou potentiels, des modalités d'utilisation commune et répétée, visant à atteindre le degré de fonctionnement optimal dans un contexte donné »* [61].

La normalisation est souvent perçue par les observateurs extérieurs comme étant un phénomène apolitique par excellence, ne rassemblant que des experts techniques en charge de développer les meilleures solutions dans leur domaine de compétence. En réalité, la normalisation, tous domaines confondus, est l'objet de rivalités de pouvoir intense entre les différentes parties prenantes qui s'y investissent, en particulier depuis son institutionnalisation par les grandes puissances industrielles occidentales à l'orée du vingtième siècle. Afin de mieux comprendre de quoi il en retourne exactement, cette première partie se divise en trois parties distinctes. La première porte sur l'histoire de la normalisation afin de mieux comprendre l'environnement actuel de la normalisation mondiale. En particulier concernant la place de la France au sein de cet environnement qui dispose d'une histoire toute particulière en la matière, qui diffère de celle des autres États européens industrialisés. Une fois l'Histoire de la normalisation abordée, la deuxième partie se concentre sur les spécificités de la normalisation des données géographiques numériques et son lien avec la cybersécurité. Enfin, la dernière partie de cette première étape de cette thèse expose les raisons pour laquelle la géopolitique s'est emparée de l'étude des processus normatifs, et comment ces derniers ce sont retrouvés au cœur de luttes de pouvoir entre États et sociétés privées pour la sécurisation des processus de productions des technologies futures. Des luttes auxquelles n'échappe pas le domaine des données géographiques numériques.

---

[60] L'Organisation internationale de Normalisation (ISO) est l'une des plus anciennes organisations internationales non gouvernementales. Fondée en 1946, elle rassemble aujourd'hui la majorité des acteurs de la normalisation dans tous les domaines techniques.

[61] ISO, « Guide ISO/IEC », partie 2, 2004, p. 4.

1. La norme, à la fois outil technique et dispositif cognitif

Le concept même de normalisation industrielle remonte à l'Antiquité, on a ainsi retrouvé des documents normatifs concernant la fabrication des clous remontant à l'Égypte antique. La conception moderne de la normalisation remonte elle à la fin du XVIIIe siècle et englobe tous les domaines industriels de l'époque. Les normes de fabrication pour des produits homogènes, tels que les textiles, les épingles et les armes à feu, ont constitué la base de la révolution industrielle de la fin du XVIIIe siècle et du début du XIXe siècle. Il est à noter à ce sujet que l'institution militaire a été la première à faire un large usage des normes, du fait de son besoin de s'appuyer sur des matériels dûment répertoriés et suivant un cahier des charges bien définis [62]. La révolution industrielle du milieu du XIXe siècle, quant à elle, a été alimentée par les progrès scientifiques dans les domaines de la chimie, de la vapeur et de l'électricité, et reposait en partie sur des standards de mesure pour un large éventail de grandeurs fondamentales, telles que le temps, la distance, l'énergie, la charge électrique et le poids atomique. La création de l'Union Internationale du Télégraphe (aujourd'hui l'Union Internationale des Télécommunications [UIT]) en 1865, puis du Comité électrotechnique internationale (IEC) en 1906, marque la naissance de la normalisation internationale moderne. Une troisième révolution, débutant au début du XXe siècle, a transformé les industries d'assemblage en utilisant des normes de compatibilité pour des dispositifs complexes, comme les voitures. Bien que des tentatives aient été faites dans les années 1930 pour élaborer des normes internationales dans d'autres domaines, ce n'est qu'après la Seconde Guerre mondiale que le Comité de coordination de la normalisation des Nations Unies, créé par les États-Unis, la Grande-Bretagne et le Canada, a lancé l'initiative qui a abouti à la création de l'Organisation internationale de normalisation (ISO) fondé en 1947 à la suite de la conférence de Londres d'octobre 1946. Enfin, la révolution des technologies de l'information et des télécommunications de la fin du XXe siècle a été diffusée en utilisant des normes d'interopérabilité [63]. Aujourd'hui la normalisation est présente partout dans notre vie quotidienne, bien que nous ne nous en rendions pas toujours compte. La meilleure illustration de cela nous vient probablement d'un message diffusé par les présidents de l'IEC et de l'ISO, ainsi que par le Secrétaire général de l'ITU, lors de la journée mondiale des normes en 1998 :

---

62 Segrestin Denis, « L'entreprise à l'épreuve des normes de marché. Les paradoxes des nouveaux standards de gestion dans l'industrie », *Revue française de sociologie*, vol. 38, 1997, pp. 38 – 39.

63 Hall Peter A. et Soskice David W., « Varieties of capitalism: the institutional foundations of comparative advantage » , Oxford , Oxford University Press, 2001.

« Bien que nous ne pensions généralement aux normes que lorsque leur absence est source d'inconvénients, il serait en fait extrêmement difficile d'imaginer la vie quotidienne sans normes. Prenez n'importe quel scénario et vous serez étonné de voir combien de normes soutiennent cet aspect de la vie quotidienne. Dès votre réveil et tout au long de la journée, les normes, sous une forme ou une autre, contribuent à façonner votre journée, à la rendre plus facile, plus confortable, plus sûre et tout simplement plus pratique. Imaginez, par exemple, que vous ne puissiez pas retirer de l'argent à un distributeur automatique de billets parce que votre carte bancaire est trop grande pour entrer dans la fente ; imaginez des piles qui ne conviennent à aucun de vos appareils électriques ; des magasins sans codes-barres pour quantifier et évaluer les stocks de marchandises ; imaginez des sites Internet sans noms de domaine normalisés. À vrai dire, une journée sans normes est inconcevable. »[64]

Les normes sont divisées en plusieurs catégories qui influent sur la façon dont elles s'imposent sur un marché. Les normes peuvent être *de jure*, c'est-à-dire approuvées par un organisme officiel de normalisation, qu'il soit national, comme l'AFNOR en France, le BSI (British Standard Institut) au Royaume-Uni ou le DIN (Deutsches Institut für Normung) en Allemagne, ou international, comme l'ISO ou le CEN (Comité européen de Normalisation) en Europe. En français, le mot « normes » est utilisé pour qualifier les normes *de jure*. Mais les normes peuvent aussi être *de facto* ou coutumières, c'est-à-dire promues par leur utilisation soit par l'industrie, comme certaines normes informatiques que le marché désigne comme étant la référence incontournable, soit par un secteur professionnel au niveau mondial ou régional, comme celle promue par l'Organisation du Traité d'Atlantique Nord (OTAN) à des fins militaires. Il arrive souvent que des normes *de facto* soient élevées au rang de normes *de jure* lorsqu'il y a un accord entre tous les partis impliqués. Le langage d'interrogation structuré (SQL) est un exemple d'une telle situation. Ainsi, en 1987, l'International Graphic Exchange Standard (IGES) qui était en compétition avec le format SQL, n'a pas réussi à devenir une norme ISO en raison de ses faiblesses dans certains domaines, tandis que le format SQL s'est imposé comme norme *de facto* [65]. Les normes sont développées dans tous les domaines de la production de biens et, selon leurs fonctions, elles peuvent également être divisées en trois catégories en reprenant la taxonomie de David (1987) [66] :

- Les normes dites de base ou fondamentales. Ces normes concernent les référentiels de terminologie, de poids et mesure ou encore de dimension. Elles permettent de fixer un

[64] IEC, ISO, ITU, 1998.

[65] Longley P A et al., « New Developments in Geographical Information Systems: Principles », *Techniques, Management and Applications-2nd edition*, 2004, p. 693.

[66] David P., « Some new standards for the economics of standardization in the information age », in Dasgupta P. et Stoneman P., *Economic Policy and Technological Performance*, Cambridge University Press, Cambridge, 1987, pp. 206 – 239.

vocabulaire commun et sont souvent des fondations essentielles à d'autres normes plus techniques. En effet, les normes de base relèvent plus de connaissances scientifiques que du savoir-faire technique.

- Les normes de qualité ou d'organisation. Ces normes sont là pour décrire les mécanismes de fonctionnement d'une entité, ou encore un seuil minimum de qualité, de sécurité ou de performance à atteindre.
- Les normes d'interopérabilité ou de compatibilité, quant à elles, définissent les conditions techniques à respecter pour rendre interopérables des produits ou systèmes.

Il faut garder à l'esprit que ces catégories ne sont pas nécessairement étanches et que certaines normes peuvent avoir plusieurs fonctions. L'existence de ces différentes catégories de normes souligne également une évolution dans les fonctions remplies par les normes durant leur histoire. Si les premières normes avaient pour soucis d'harmoniser et de rationaliser la production de biens, à commencer par l'emploi d'unité de mesure précise, d'autres fonctions sont apparues. L'attention des industriels au tournant du XXe siècle s'est ainsi tournée vers la normalisation de la qualité des produits finis et non uniquement vers la rationalisation du processus de fabrication. Aux préoccupations concernant la qualité des produits se sont ajoutées celles concernant la qualité de l'ensemble du processus de production, comme l'illustre la naissance de la série de normes ISO 9000 créée en 1987[67]. Enfin, le développement de l'informatique a propulsé une forte demande concernant des normes d'interopérabilité visant à répondre aux problèmes posés par le nombre croissant d'incompatibilités techniques entre différents systèmes informatiques. Une catégorie de problème qui s'est largement étendue avec l'irruption d'Internet et le développement du cyberespace.

Les normes remplissent donc différents rôles et contiennent des informations plus ou moins contraignantes pour les parties prenantes du domaine auquel elles s'appliquent. Ainsi, les normes de base sont là pour définir des règles qui doivent être suivies et des codes essentiels à la compréhension du domaine technique en question. De fait, ces normes doivent être connues et appliquées par l'ensemble des acteurs de la communauté scientifique auquel elles se rapportent. Les normes d'interopérabilité, quant à elles, se contentent d'énoncer les règles minimums pour garantir l'interconnexion entre différents produits ou services. Par conséquent leur *« dimension prescriptive »* [68]est très faible. À moins que des États rendent obligatoires ces normes par le biais de lois ou de décrets, ces normes sont systématiquement volontaires. Enfin, les normes de qualité se situent entre ces

[67] ISO 9000 : systèmes de management de la qualité - principes essentiels et vocabulaire.

[68] Benezech Danièle, « La norme : une convention structurant les interrelations technologiques et industrielles », *Revue d'économie industrielle*, vol. 75, Normalisation et organisation de l'industrie., 1er trimestre 1996, pp. 27 – 43.

deux catégories en matière de dimension prescriptive. Si elles restent par défaut toujours volontaires, les normes de qualité sont très souvent traitées par les acteurs de la normalisation comme étant de facto obligatoire dans un domaine une fois publier. En effet, la conformité à une norme de qualité permet de recevoir une certification, un effet très recherché par les industriels, en ce qu'elle leur permet de communiquer immédiatement auprès des autres acteurs des informations concernant la qualité de leur produit et/ou de leurs processus de fabrication. La norme a donc une dimension cognitive qui va au-delà d'un but purement technique d'harmonisation des moyens de production, en étant un vecteur d'information dirigé vers les autres acteurs de la normalisation, des industriels aux consommateurs. La norme est toujours produite et assimilée au sein d'une communauté précise qui peuvent être circonscrite par des limites géographiques précises, par exemple dans le cas de normes nationales imposées par certains États, comme cela a longtemps été le cas avant l'internationalisation de la normalisation, où au contraire de façon transnationale comme cela arrive désormais quasiment systématiquement dans le cadre d'une économie mondialisée, au sein de secteurs industriels entiers sans regard pour des limites géographiques. Cependant, si la dimension géographique de l'application des normes techniques est de moins en moins prévalente du fait de l'ouverture de l'économie mondiale, le développement des normes continue d'être régi par des logiques géographiquement marquées, et ce, à toutes les échelles de développement.

De fait, la norme est aujourd'hui un outil essentiel de l'économie mondiale, et ce, dans tous les domaines techniques. Englobant l'ensemble des secteurs de l'économie, la normalisation rassemble un très grand nombre d'acteurs aux logiques parfois divergentes concernant les raisons de leur implication : entreprises privées, États, organisation internationale, consortiums privés, associations de consommateurs, universités, etc. Comme le souligne l'étude monographique menée par trois politologues français [69], la connaissance des relations de pouvoir qui lient les acteurs de la normalisation internationale et les stratégies qu'ils mettent en place reste un domaine encore peu étudié, malgré l'existence de certaines études pionnières en la matière, en particulier dans le domaine de l'économie politique. Comme nous l'avons vu précédemment, la normalisation s'est internationalisée et institutionnalisée à la fin de la Seconde Guerre mondiale et a directement participé à la mondialisation de l'économie et à la diffusion du modèle de production capitaliste qui domine aujourd'hui l'économie mondiale. La libre circulation des biens et des personnes a été rendue possible par la mise au point de politique internationale en matière de normalisation conçue par un ensemble d'acteurs institutionnels internationaux qui se sont appuyés sur des normes pour régler les échanges

[69] Dudouet et coll., « Politiques internationales de normalisation » quelques jalons pour la recherche empirique », *revue française de science politique*, vol. 56, 2006, p. 367 – 392.

internationaux. Les recherches en économies soulignent souvent [70] que la normalisation est très tôt rentrée en ligne de compte comme un élément de la compétition entre sociétés privées comme des facteurs d'acquisition d'un avantage compétitif sur la concurrence en favorisant l'innovation.

En permettant la diffusion d'informations et, par là, en contribuant à l'accroissement des connaissances collectives, la norme constitue un *« dispositif cognitif collectif »* pour reprendre les termes de l'économiste Olivier Favereau (1989)[71]. C'est-à-dire que la diffusion des normes participe à la création d'un dispositif d'anticipation mutuelle fondé sur l'acceptation par l'ensemble des participants de règles et de contraintes édictées par les normes. La norme est donc à la fois un outil destiné à répondre à une problématique précise et une recommandation (pas nécessairement suivi puisque majoritairement non obligatoire) qui est utilisée par l'ensemble des parties prenantes pour contourner leur propre ignorance sur un sujet ou un procédé particulier. Les normes participent ainsi du développement d'une *« économie de savoir » »*[72] ,car elles sont librement diffusées et participent à modeler les comportements collectifs entre sociétés et entre individus dans le domaine de la production de biens et de savoirs. Ainsi, même si les normes ne sont que très rarement imposées, elles ont un fort pouvoir conventionnel en servant de repère pour juger de la qualité d'un bien produit et participent directement de la façon dont sont conçus les technologies présentent et futures. La norme influe donc directement sur le phénomène « *d'asymétrie de l'information »* décrit par Akerlof (1970)[73] qui souligne que l'incertitude concernant la qualité d'un produit influe fortement sur les comportements des acheteurs potentiels. À ce titre, les normes, en apportant des garanties de fabrication et/ou de qualité, participent directement du succès des produits qui s'y rapportent sur le marché en offrant des informations supplémentaires aux acheteurs qui réduisent l'asymétrie de l'information. À ce sujet, il faut également distinguer les normes des conventions de qualité, qui ne sont pas nécessairement des normes. Le premier objectif d'une convention de qualité est d'offrir un moyen d'assurer une coordination entre plusieurs producteurs d'un minimum qualité autour d'un produit, et par là de réduire le degré d'incertitude concernant les caractéristiques d'un produit. La principale différence avec une norme est que la convention de qualité se repose sur un ensemble d'acteurs extérieurs aux producteurs, qui sont en charge de juger *a posteriori* de la qualité du produit. Une norme au contraire, s'inscrit dans le processus de production du bien, et n'est pas imposée par un acteur extérieur, mais est auto-imposée par le producteur. Comme le souligne Benezech (1996),

---

70 Matutes Carmen et Regibeau Pierre, « A Selective Review of the Economics of Standardization : Entry Deterrence, Technological Progress and International Competition », *European Journal of Political Economy*, vol 12, 1996, pp. 183 – 209.

71 Favereau Olivier, « Marchés internes, marchés externes », *Revue économique*, vol 40, n° 2, 1989, pp. 273 – 328.

72 *Ibid*

73 Akerlof George, « The Market for "Lemmons" : Quality Uncertainty and the Market Mechanism », *Quarterly Journal of Economic*s, n° 84, p. 488 – 500, 1970.

> *« (…) l'existence d'une norme, donc de produits certifiés conformes, a des répercussions ex ante sur les conditions d'échange. Elle influence les préférences et la réalisation du contrat marchand, puisqu'une condition de réalisation de ce contrat peut être une référence aux normes existantes ou une exigence de certification. Dans ce dernier cas, la réalisation même de l'échange dépend de l'existence d'un contrat préalable, passé entre l'organisme certificateur et le producteur. La norme n'est donc pas un intermédiaire extérieur aux contractants, puisque sa prise en compte résulte d'une décision intentionnelle de ceux-ci. C'est un critère d'évaluation, construit collectivement et utilisé individuellement par les contractants, avant ou pendant la réalisation de l'échange » »*[74].

La nature structurante de la norme et son influence sur le développement de produits tiennent donc au fait qu'elle naît d'un travail collectif de recherche d'un consensus qui implique toutes les parties prenantes. Cependant, il est souvent observé qu'une partie des parties prenantes, notamment les utilisateurs finaux, sont rarement présentes dans les processus de négociations, de la même manière que les TPE sont souvent absentes également. Cette observation renforce l'idée que la normalisation est un processus avant tout défini par les acteurs qui y prennent part, moins que par des injonctions institutionnelles. La légitimité du processus normatif, si elle est souvent bâtie en partie sur l'ancienneté des organisations internationales de normalisation, provient avant tout de l'intérêt qu'y prêtent les acteurs de l'industrie, qui, par leur participation, augmente les chances que les consensus établis dans ces organisations soient fondés sur un large accord des parties prenantes. Les normes ont un pouvoir de codification et de limitation des possibles en participant de l'émergence de technologie dominante au sein des marchés. Le développement de certaines normes de base, comme les normes métrologiques, à des répercussions sur les évolutions technologiques futures dans le domaine technologique auquel elles s'appliquent. Ces normes sont érigées en référentiels techniques essentiels qui influent sur la construction de l'architecture technique dont elles constituent les fondations. Dans ce sens la norme participe de la structuration des possibles.

Il existe donc une relation de symbiose entre les acteurs de l'industrie et les organismes de normalisation, les premiers tirent des normes des garanties de diffusion de technologies et de modes de production qui ont leurs faveurs, tandis que les organismes de normalisation tirent leur légitimité de la participation de ces mêmes acteurs. Ainsi, plus la participation des parties prenantes est large, plus la légitimité de la norme est garantie, assurant à son tour sa diffusion et son impact normatif sur le développement de l'industrie. La capacité à influer sur la production de certaines normes peut avoir des

[74] Benezech Danièle, « La norme : une convention structurant les interrelations technologiques et industrielles », *Revue d'économie industrielle*, vol. 75, Normalisation et organisation de l'industrie., 1er trimestre 1996, P. 34.

conséquences à long terme très importantes, ce qui justifie de la compétition internationale qui se joue dorénavant au sein des institutions internationales de normalisation dans tous les domaines techniques.

1.1 Quelle Géographie pour la normalisation ?

La normalisation technique est aujourd'hui l'enjeu de luttes de pouvoir intenses mêlant États et firmes privées pour le contrôle de l'innovation technologique de demain, notamment dans le domaine des données géographiques numériques. En cela, la compétition en matière de normalisation constitue un des enjeux géopolitiques du monde moderne. Nous nous appuierons ici sur la définition de la géopolitique donnée par Paul Claval dans son ouvrage *Les espaces de la politique* (2010) afin de développer plus avant en quoi cette dernière s'applique au champ de la normalisation des données géographiques :

> *« La géopolitique analyse les réalités géographiques dans lesquelles des rapports de pouvoir (coercition, influence, domination, contrôle) naissent de l'accès à certaines ressources et sont liés à leur mise en valeur et leur utilisation. Elle part des acteurs. Ceux-ci sont localisés, s'appuient sur des bases territoriales, disposent de réseaux : on ne peut les comprendre sans tenir compte de leurs dimensions géographiques. La géopolitique décrit le théâtre où les acteurs s'affrontent, présente la scène des opérations, la disposition des ressources qui sont contrôlées par les uns et les autres, et la localisation de celles qui sont l'objet du litige. Elle envisage les forces engagées dans la confrontation, les manœuvres que conçoivent les partis. Les décisions que prennent les acteurs étudiés par la géopolitique résultent de l'analyse qu'ils font de la situation et des idées qui transparaissent dans leurs décisions. Ce sont celles que partagent les groupes auxquels ils appartiennent. L'image qu'ils se font de ce qu'est une ressource, de ce qu'elle peut rapporter et de la meilleure manière de la contrôler et de la mettre en valeur compte également »*[75].

Tout d'abord, concernant l'aspect géographique, si la normalisation peut apparaître au premier abord comme territorialisée, se bornant uniquement à un enchaînement de discussions techniques ayant de plus en plus souvent lieu virtuellement, la réalité est tout autre.

La normalisation se divise en diverses arènes, qu'on peut découper en trois grandes échelles géographiques, que sont l'échelle internationale, continentale et enfin l'échelle nationale. Ces différentes échelles sont interconnectées avec une intensité variable en fonction des acteurs qui y

[75] Claval Paul, « Les espaces de la politique, », Paris, Armand Colin, mai 2010, pp. 15 – 16.

prennent part. Ainsi, pour les acteurs européens, l'échelle continentale est une composante essentielle de tout processus de normalisation de par l'importance de la production de normes à cette échelle au sein du Comité européen de Normalisation (CEN)[76] et du Comité européen de Normalisation pour l'Électrotechnique (CENELEC)[77], ainsi que par la préséance des lois européennes sur les lois nationales, qui font que les règles de normalisation européennes s'appliquent à tous les États membres de l'Union. La situation de l'Union européenne en la matière est sans équivalent dans le monde. Si plusieurs organisations régionales disposent d'organisations jumelles centrées sur la normalisation, ces dernières se contentent généralement d'apporter un avis purement consultatif ou se concentrent sur des domaines techniques limités. Par exemple, l'Association des nations de l'Asie du Sud-Est (ASEAN) dispose de sa propre organisation internationale de normalisation, le Comité consultatif de l'ASEAN pour les normes et la qualité (ACCSQ). Contrairement au CEN/CENELEC, les décisions de l'ACCSQ ne se surimposent pas aux lois des pays membres de l'ASEAN, et reposent sur la bonne volonté de ces derniers pour être appliquées. Dans le même ordre d'idée, la Ligue arabe dispose de sa propre organisation régionale de normalisation, l'Organisation arabe pour le développement industriel, la normalisation et l'exploitation minière (AIDMO). Cependant, contrairement aux instances européennes, cette organisation concentre l'essentiel de ses activités dans le secteur minier. Ainsi, l'Europe est le seul continent qui dispose d'organisations de normalisation dont les décisions sont soutenues par des lois d'application obligatoire, tout du moins pour les pays membres de l'Union européenne (UE).

Ainsi, l'implantation géographique d'un acteur va jouer un rôle direct sur son implication dans le différent processus normatif auquel il souhaite participer. L'échelle internationale occupe indéniablement une place maîtresse dans le domaine de la normalisation technique, via des organismes internationaux comme l'ISO ou des consortiums privés, comme l'OGC. Cela tient au fait qu'une grande partie des normes produite aux échelons géographiques inférieurs consistent en une application de normes développées à l'échelle internationale afin de rester en conformité avec les derniers développements en la matière. À l'échelle régionale, ces choix peuvent s'accompagner d'une sélection en matière d'application de certaines normes (tous les aspects d'une norme ne sont pas d'application obligatoire), et ont pour but de participer à la diffusion au sein du groupe régional de ces nouvelles normes internationales. À l'échelle nationale, seuls les acteurs nationaux impliqués dans le processus

[76] Le CEN est une association internationale qui fournit une plateforme pour l'élaboration de normes européennes et d'autres documents techniques relatifs à divers types de produits, matériaux, services et processus.

[77] Le CENELEC soutient les activités de normalisation dans un large éventail de domaines et de secteurs, notamment : Compatibilité électromagnétique, accumulateurs, piles primaires et batteries primaires, fils et câbles isolés, équipements et appareils électriques, fournitures électroniques, électromécaniques et électrotechniques, moteurs et transformateurs électriques, équipements d'éclairage et lampes électriques, matériel pour installations électriques basse tension, véhicules électriques, chemins de fer, réseaux intelligents, comptage intelligent, systèmes d'électricité solaire (photovoltaïque), etc.

de production de normes participent à leur création et ces dernières ne s'appliquent qu'aux acteurs nationaux. Là encore, certaines normes nationales servent à imposer aux acteurs nationaux l'application de normes régionales, comme cela est souvent le cas en Europe. Cependant le développement de normes nationales spécifiques, qui se concentrent généralement sur des domaines précis relevant de l'autorité de l'État, peut également aboutir au développement de normes originales visant à répondre au mieux aux besoins des acteurs nationaux décorrélés des normes internationales dans le domaine. Ces trois échelles interagissent donc entre elles à la façon de vase communicant, où l'échelon international rassemble généralement les acteurs les plus innovants et les travaux les plus nombreux (car il rassemble souvent les acteurs qui ont la capacité d'investissement en personnel et en argent la plus importante) dans un domaine, dont les normes vont en quelque sorte « ruisseler » aux échelons régionaux et nationaux en engendrant le développement de normes originales visant, à chaque échelon, à répondre aux besoins des acteurs impliqués dans ces processus.

La nature des acteurs joue également un rôle fondamental dans la façon dont ces derniers interagissent et participent aux processus normatifs. Ces derniers se répartissent en plusieurs catégories qui sont les États et leurs représentants issus de leurs organismes nationaux de normalisation, les sociétés privées et enfin les consommateurs et leurs syndicats. Si tous les échelons rassemblent à différents degrés l'ensemble de ces types d'acteurs, tous n'y participent pas selon les mêmes modalités et avec la même intensité. À l'échelle internationale, il faut différencier les acteurs nationaux qui développent des normes au sein de l'ISO et les acteurs privés qui se rassemblent en consortiums. En effet, les acteurs privés n'ont pas de droit de vote à l'ISO où ne sont représentés que les États. Cependant, les firmes peuvent tout de même faire entendre leurs voix, soit par le biais de leurs représentations nationales, qui ont également en charge de porter leurs revendications à l'international, mais également à travers des organismes de liaison qui existent au sein de chaque comité technique de l'ISO pour permettre le dialogue entre l'ISO et les consortiums privés. Ces consortiums, quant à eux, sont le lieu du développement des normes par les acteurs privés. Cependant, les consortiums étant dépendant financièrement de la participation de leurs membres, ces derniers exigent généralement un paiement et classent leurs différents membres en fonction de leur contribution financière. En effet, être capable de participer financièrement de façon importante au fonctionnement d'un consortium de normalisation, comme l'Open Geospatial Consortium (OGC) donne accès à certains avantages. Peut ainsi être cité, à titre d'exemple : siéger au sein du comité stratégique de l'OGC ou encore mobiliser des experts internationaux pour concevoir des solutions répondant à ses besoins spécifiques[78].

De ce fait, les petites et moyennes entreprises sont rarement membres de consortiums privés qui rassemblent avant tout les géants de leurs industries respectives, les premiers participant plus volontiers

[78] Site Internet de l'OGC : https://www.ogc.org/join/

aux travaux de normalisation uniquement à l'échelle nationale qui ne nécessite pas de participation financière. Ainsi, même s'il existe de fortes interconnexions entre les différentes échelles de la normalisation, ces dernières restent assez étanches pour ceux qui n'ont pas la possibilité, les moyens et/ou le temps d'être membres de l'ensemble des arènes de la normalisation. Au contraire, certains acteurs, notamment ceux nommés par les instances nationales de normalisation, se meuvent de façon beaucoup plus fluide au sein des différentes arènes de la normalisation, et il n'est pas rare pour un expert de l'IGN, par exemple, de participer au développement de normes internationales, puis à la modalité de leur application à l'échelle régionale avant de s'intéresser au développement de normes similaires à l'échelle nationale ou inversement. Ces mêmes personnes sont également amenées à travailler dans différents domaines couverts par les normes de leur domaine technique, comme dans le cas des données géographiques numériques qui disposent de circuits distincts en matière de normalisation dans le monde civil et militaire, mais qui rassemblent souvent les mêmes spécialistes dans ces deux domaines. Le nombre relativement faible d'individus travaillant dans le domaine de la normalisation des données géographiques numériques renforce l'importance des réseaux interpersonnels tissés par ces experts dans l'exercice de leur métier. La constitution de ce capital social au sein des instances de normalisation est presque aussi importante que le capital technique pour l'expert. En effet, dans ce milieu de la normalisation où le consensus, et par extension, la négociation, est au cœur du processus de fonctionnement, les relations humaines que l'expert entretien joue également dans sa capacité de négociations. Ces connaissances constituent un capital social constitué par l'expert qu'il réinvestit en participant aux négociations au sein des organisations de normalisation. C'est également un capital qu'il peut vendre en étant employé par des sociétés ou d'autres organismes de normalisation désireux d'employer son expérience.

Avec la création de l'ISO au sortir de la Seconde Guerre mondiale, la majorité des pays industrialisés, et, avec eux, leurs firmes, ont perçus un intérêt majeur dans la coopération industrielle. Les raisons de coopérer avec d'autres firmes, nationales ou étrangères peuvent être multiples et plusieurs théories concernant l'innovation et l'investissement en Recherche & Développement (R&D) ont été développés à ce sujet. Le choix d'investir ou non dans la normalisation est souvent dicté pour les firmes par le prix du « ticket d'entrée » et d'une estimation relative de la force de la concurrence dans son domaine d'activité[79]. En d'autres termes, soit, la société considère qu'elle est déjà en position de monopole et que la norme va permettre de formaliser une domination déjà acquise de facto, ou qu'au contraire, la coopération industrielle avec d'autres normes est une opportunité de renforcer ses potentielles parts de marché en développant un produit adossé à une norme reconnue dans un contexte

[79] Stanley M. Besen et Farrell Joseph, « Choosing How to Compete : Strategies and Tactics in Standardization », *Journal of Economic Perspectives*, n° 8, 1994, pp. 117 – 131.

où elle ne peut espérer acquérir un monopole. Face à la multiplication des concurrents potentiels dans le contexte de l'ouverture de l'économie mondiale post Seconde Guerre mondiale, en particulier en Occident, nombreuses furent les sociétés à reconsidérer l'intérêt de la normalisation pour le développement de leurs produits, avec ou sans incitation étatique à le faire. La formation de telles coalitions d'intérêts parmi les firmes permet souvent l'émergence d'une norme dominante, mais pas nécessairement de la meilleure norme techniquement parlant, comme le soulignait déjà une enquête de l'OCDE en 1991[80]. Cela s'explique principalement par la recherche d'un avantage oligopolistique de la part de certaines firmes participant à ces processus, qui peut se faire aux dépens du consommateur, en particulier lorsque ces derniers ne participent pas aux négociations. Ainsi, la normalisation fait partie intégrante des stratégies d'entreprises et constitue une des variables essentielles de la compétition internationale.

Le rôle que jouent les normes et les questions liées aux normes dans le commerce a été de plus en plus reconnu au fil du temps. Il a été reconnu que la négociation et l'adoption de normes techniques pour toutes les catégories de produits et de services peuvent conduire à la formation de coalitions économiques et politiques entre les nations et les régions et à la segmentation du marché entre les principaux producteurs. La normalisation dans certains domaines techniques peut avoir des conséquences géographiquement très marquées. Ainsi, dans le domaine des chemins de fer, la normalisation des rails participe à découper des espaces normatifs distincts à la surface du globe. Même en Europe, où la question de la normalisation des infrastructures est prise très au sérieux, la normalisation des rails reste un casse-tête sans solution apparente[81]. De plus, historiquement, la surreprésentation des pays occidentaux au sein des instances de normalisation internationales découpe un monde de la normalisation séparé sur le mode centre-périphérie, où, là encore, l'occident concentre les membres fondateurs et les plus actifs, et où les pays du Sud global restent pour la majorité des périphéries de la normalisation internationales. Ces derniers participent au processus normatif de façon inversement proportionnel à l'importance de leur population. Les groupes nationaux et régionaux motivés par des intérêts concurrents peuvent utiliser les réglementations et les normes à des fins politiques. Les entreprises comme les États utilisent les normes pour réduire les coûts de transaction internes et externes, pour faire baisser les prix des fournisseurs, pour bloquer ou contourner les concurrents, pour exercer un plus grand contrôle sur les employés, les fournisseurs et/ou les clients, et pour établir des références pour des cycles d'innovation ultérieurs. Les économies d'échelle, de vitesse

[80] OCDE, « La dimension économique des normes en matière de technologies de l'information », Paris, OCDE, 1991.

[81] Ainsi, si la plupart des pays européens ont adopté l'écartement dit standard des rails de 1 433 mm, ce n'est pas le cas de tous. La péninsule ibérique a conservé son propre écartement de rails de 1 666 mm. Tandis que certains pays de l'ex-bloc soviétique utilisent toujours l'écartement russe de 1 520 mm. Kemmeter (de) Frederic, « Des différences d'écartement de voies en Europe ? Pas autant qu'on ne le croit », Le Rail, 6 mai 2022.

et de qualité dépendent toutes de l'utilisation de normes. Les stratégies échafaudées par les différents acteurs dans leur quête de contrôle du processus normatif reposent également sur les représentations qu'ils se font de leurs forces et faiblesses, qui guident leur propension à s'allier à d'autres acteurs pour collaborer au développement d'une norme ou au contraire à chercher un monopole par le biais de la diffusion d'une norme précise dont ils auraient guidé la conception.

1.1.1 Normalisation des données géographiques numériques et souveraineté

Dans le domaine de la géographie, le rôle des normes est également ancien et revêt d'une importance particulière non seulement pour les acteurs de l'industrie, mais également pour les États. Comme indiqué plus haut, la première institution à s'être intéressée de près à la normalisation est l'institution militaire, et cela vaut également pour les normes géographiques. Il faut attendre l'époque moderne pour voir se constituer les premiers dépôts de cartes se fait sous l'impulsion de l'institution militaire à des fins de connaissance du territoire en vue de sa défense. Ainsi, dans le royaume de France, le dépôt de la guerre est créé en 1688 et vise à conserver toutes les cartes connues, nationales ou étrangères utiles à la défense du royaume. Cependant ces premières cartes ne relèvent pas encore d'un effort de normalisation des productions, mais uniquement d'accumulation d'un savoir que l'on sait depuis longtemps essentiel à la défense du territoire. Le corps des ingénieurs géographes est formé quant à lui en 1726 et amorce la professionnalisation de la production cartographique pour les armées. Il faut cependant attendre le lendemain de la Révolution française pour voir émerger en 1791 un véritable effort de normalisation des données géographiques militaires. Ainsi, comme le note Philippe Boulanger dans son ouvrage *La géographie reine des batailles* (2020),

> *« L'adoption du système métrique et de l'échelle décimale en 1791, qui permet de calculer la méridienne de Cassini de Dunkerque à Barcelone entre 1792 et 1798, la codification et l'uniformisation des cartes à partir des travaux de la commission de topographie, créée en 1802, enfin la mise en place des bureaux militaires de topographie renforcent la tendance à la rationalisation des modes de production centralisée du Dépôt de la guerre. Sont adoptés des signes conventionnels, les cotes d'altitude par rapport au niveau de la mer, le dessin en « éclairage oblique », le hachurage perpendiculaire aux courbes de niveau pour préciser le relief, la projection Bonne pour conserver les surfaces (les méridiens sous forme de courbes concourantes) »*[82].

[82] Boulanger Philippe, « La géographie reine des batailles », Perrin, p. 26 – 27, 2020.

Le développement de la science géographique doit donc beaucoup à l'institution militaire qui constitue une des premières communautés au sein de l'État français à saisir l'importance de la maîtrise du savoir géographique et de sa normalisation. Un phénomène que l'on retrouve également au sein de toutes les nations modernes occidentales dès le XIX siècle, à l'exemple de la Prusse qui dote son état-major d'un corps de géographe dès 1816. La normalisation de ces données est un élément capital de leur diffusion et de leur utilisation, en organisant le savoir géographique en produits cartographiques cohérents, immédiatement employable comme outil d'aide à la décision. De plus, la géographie étant une science au carrefour des sciences humaines et des mathématiques, elle offre à l'État bien plus qu'une connaissance de sa géographie physique, mais également des outils d'analyse précieux sur les dynamiques qui animent sa population. La normalisation des produits cartographiques rend l'ensemble des cartes produites interopérables et facilite leur diffusion. L'édiction de normes et la diffusion du savoir géographique ont également permis la multiplication des travaux cartographique sur tout le territoire national, mais également sur les territoires occupés lors des conflits qui ont suivi, notamment sous le Directoire et le 1er Empire. Le XIXe siècle a également été un siècle riche de production géographique également hors de l'Europe, où les puissances coloniales se sont mises à produire des cartes en Afrique et en Asie sur des espaces autrefois très mal connus des Européens. C'est également une période où d'autres États non européens développent leur propre savoir géographique sur leur territoire, mais également au-delà. Le Japon impérial étant dans ce domaine une des Premières Nations non occidentales à créer sa propre école de géographie, puis de géopolitique, et à développer ses propres normes en la matière dès 1890[83].

L'importance que les États modernes ont placée très tôt dans la production de données géographiques va cependant au-delà du simple besoin de mener les affaires militaires. Pour reprendre la définition désormais célèbre que Max Weber donne de l'État, *« L'État est cette communauté humaine, qui à l'intérieur d'un territoire déterminé (…) revendique pour elle-même et parvient à imposer le monopole de la violence physique légitime »*[84].

Il est intéressant de noter, comme le souligne Marian Eabrau (2012) que *« seule la définition wébérienne sert désormais de référence pour les études, notamment en science politique, qui mobilisent la notion d'« État » »*[85]. Sa définition est un parfait exemple de norme de facto en Science politique. Ainsi, cette dernière, même si elle n'est pas exempte de critique, a fini par s'imposer par l'immense popularité au sein de l'institution scientifique qu'est la Science politique, de l'ouvrage de Weber. Que

---

83 Au sujet du développement de la géographie et de la géopolitique japonaise, voir l'ouvrage de Pelletier Philippe, « La Japonaise. Géopolitique et géographie historique de la surinsularité au Japon », Paris, CNRS éditions, 1997.

84 Weber Max, « Le savant et le politique » in « La politique comme profession et vocation », Paris, La Découverte, p. 118, 2003.

85 Eabrau Marian, « Les États de la définition wébérienne de l'État », *Raisons politiques*, n° 45, p.187, 2012.

la popularité de la définition donnée par Weber justifie a posteriori de la justesse de cette même définition ne doit pas être présupposé. C'est ce qui permet notamment aux chercheurs de l'épistémologie de la science politique de continuer à critiquer cette théorie. Ainsi, il est important de garder à l'esprit que l'imposition d'une norme est avant tout un marqueur de l'émergence d'une opinion dominante concernant la solution à un problème posé, et ne doit pas être comprise comme une preuve sans équivoque de l'efficacité de la solution proposée. La notion wébérienne d'État, si elle a le mérite de poser les bases sur lesquels ils se fondent, nécessite d'être étendue. En effet, les prérogatives de l'État contemporain ne se limitent pas uniquement à garantir les fonctions de base dudit État. Le développement dans la seconde moitié du XXe siècle du concept « d'État providence » a fait évoluer la perception des populations occidentales sur le contrat social qui lie les individus à leur État, allant pour ce dernier au-delà de la simple protection des individus et des échanges commerciaux. Cette notion induit que l'État moderne se doit également de fournir à ses citoyens un certain nombre de services qui ne peuvent pas être fournis par le marché[86]. L'imposition et la diffusion de normes par l'État sont un des outils à sa disposition pour assurer à ses administrés un certain nombre de ces services, en imposant aux acteurs du marché un certain nombre d'exigences visant à garantir la protection de la santé et de la sécurité des citoyens et/ou la protection de leur environnement. L'État providence se doit de s'occuper également du bien-être de ses citoyens, une notion qui rentre en ligne de compte lorsque l'on s'intéresse au rôle joué par la diffusion, rendu possible par la normalisation, des données géographiques et leur usage par la puissance étatique.

Un autre élément de la définition wébérienne de l'État à analyser est le concept de légitimé qui est rattaché à l'exercice de la violence. Ainsi, un État ne peut être défini comme tel que s'il réussit à faire percevoir comme légitime auprès de ses administrés l'exercice de la violence dont il a le monopole. Cette légitimité peut s'acquérir de plusieurs façons. Weber fait la différence entre plusieurs modes d'autorité. L'autorité « rationnelle » qui provient de la reconnaissance par la population de la légitimité du droit qui institue par écrit la légalité de l'autorité de l'État. L'autorité traditionnelle qui s'appuie sur l'ancienneté de la tradition et la sanctification de cette dernière comme règle mesurant la légitimité des dirigeants qui s'en revendiquent. Enfin, la notion de charisme qui fonde la soumission des citoyens à l'autorité de l'État sur le caractère exceptionnel de la personne en charge de la conduite de l'État[87]. Cette quête de légitimité de l'État peut être mise en parallèle avec l'autorité des organismes internationaux de normalisation et des consortiums privés dont la légitimité se transmet aux normes qu'ils produisent, que ces dernières soient soutenues par des législations ou non. Ainsi, le problème de la légitimité de la norme anime tous les groupes de production de normes. Dans le cas de l'ISO, cette

[86] Von Hayek Friedrich, « Droit, législation, liberté », in *L'ordre politique d'un peuple libre*, Vol. 3, Paris, PUF, 1983.
[87] Weber Max, « Économie et société », tome 1, Paris, Plon, 1995.

dernière tire sa légitimité non seulement de son ancienneté, mais aussi d'une forme d'autorité rationnelle qu'elle tire du respect de ses principes de fonctionnement fondé sur la recherche permanente du consensus, fixés par écrit dans ses statuts. Enfin, l'adhésion massive des organes nationaux de normalisation à travers le monde aux principes de fonctionnement de l'ISO et leur participation quasi universelle a permis de cimenter la légitimité des normes ISO depuis 1947. Si cette confiance dans les procédures de l'ISO venait à s'effriter et, avec elle, la participation des organismes nationaux, la légitimité des normes produites par l'ISO s'en voyait immédiatement annihilée, et ce, indépendamment de la justesse des solutions techniques proposées. Autrement dit, il ne faut pas sous-estimer le rôle du discours et des représentations attachés au fonctionnement des organismes de normalisation dans la façon dont les différents acteurs concernés s'attachent aux organismes de normalisation et aux normes qu'ils produisent. La légitimité de l'organisme de normalisation est une condition *a priori* de la réussite d'une norme, et c'est avant tout parce que l'organisme de normalisation est perçu comme légitime et fonctionnant selon des principes censés que les normes qu'il produit sont approuvées par la communauté internationale.

Une des conditions sine qua non de l'existence de l'État est donc sa capacité à être délimitée dans l'espace, de posséder des frontières au sein desquels la structure étatique exerce un pouvoir dominant, revendiqué ou tout du moins accepté par les individus qui en sont les administrés. L'État tire sa légitimité de sa capacité à maintenir ses prérogatives régaliennes (assurer la sécurité intérieure et extérieure, définir le droit et rendre la justice, frapper monnaie et définir le budget de l'État) sur un territoire donné. Les données géographiques sont définies par l'Institut géographique national (IGN) comme, *« toute donnée faisant directement ou indirectement référence à un lieu spécifique ou une zone géographique »*[88]. Elles sont pour l'État en tant que structure dominante une importance capitale, car leur acquisition est la condition sine qua non de la connaissance objective d'un territoire dont la protection fait partie des fondements de sa légitimité, en ce qu'il est l'espace sur lequel s'exerce sa souveraineté. Il n'est pas d'État sans territoire. La diffusion des données géographiques et leur réutilisation par le biais des administrations de l'État à travers les politiques publiques d'aménagement du territoire ou encore les projets portés par des sociétés privées remplissent également pour l'État la fonction de construire une image du territoire sur lequel il règne auprès de sa population et des pays étrangers. Les informations géographiques sont définies par l'IGN comme toute *« information qui est reliée à une localisation sur la Terre, exprimée par rapport à un système de référence. Une information géographique est une information que l'on peut situer sur un plan, une carte, directement par des coordonnées ou indirectement par relation à une autre information géographique. C'est, en particulier,*

[88] Glossaire de l'information géographique de l'IGN : https://www.geoinformations.developpement-durable.gouv.fr/glossaire-de-l-information-geographique-a855.html

l'information sur les objets ou phénomènes naturels, les ressources culturelles, humaines ou économiques »[89].

La normalisation des données géographiques sert non seulement à faciliter la production des outils cartographiques de toute nature (cartes topographiques, politiques, couverture Lidar[90], carte hydrographique, etc.), mais également à fixer un vocabulaire visuel par le biais des codes de la sémiologie graphique afin de projeter auprès des populations des représentations du territoire qu'elles habitent pour mieux imprégner ces populations de la conscience de la communauté politique auxquelles elles appartiennent. Les données géographiques sont donc un outil dans l'arsenal de l'État pour l'exercice non seulement de la violence physique dont il a le monopole par la cartographie et le contrôle du territoire, mais également comme outil de violence *symbolique* dont il ne dispose pas du monopole[91], par le biais des représentations qu'elle aide à diffuser au sein des populations. Ainsi, la représentation cartographie fait partie des éléments de langage qui assoient la domination de l'État sur ses administrés, en donnant à voir à tout instant l'étendue de l'autorité de l'État, systématiquement présenté comme un continuum lisse effaçant du même coup les disparités éventuelles en termes de contrôle réel de l'État sur ledit territoire. Cette dernière participe également à *naturaliser* auprès des populations ses subdivisions territoriales et administratives, toujours artificielles, tout en constituant un outil essentiel de leur aménagement. Jamais la puissance de l'État n'est aussi bien mise en valeur que dans les atlas. À titre d'exemple, la République populaire de Chine n'hésite pas à publier des cartes officielles où ses frontières s'étendent sur des territoires officiellement revendiqués par ses voisins[92]. La projection de la puissance réelle ou supposée passe aussi par la diffusion de données géographiques. C'est dans ces cartes, et dans les innombrables choix qui président à leurs créations (projection, symbologie, couleurs, graphie) que la puissance de l'État est le mieux mise en valeur. En constituant un moyen passif d'affirmation du pouvoir de l'État, tout en appelant les citoyens sujets à incarner cette communauté politique contenue dans ces frontières ainsi exposées et par là même à le servir, les données géographiques font donc bien parti d'un outil de l'exercice de la violence *symbolique* dont peut user l'État au sens que lui donne Bourdieu, en ce qu'elle participe à renforcer l'approbation implicite des citoyens au monopole de la violence physique légitime de l'État sur cet espace. La

---

89 *Ibid*

90 Light détection and ranging (Lidar) ou détection et télémétrie par la lumière sont une technologie de télédétection optique qui mesure les propriétés absolues d'une lumière diffusée, y compris la portée, à partir de laquelle des données d'élévation sont dérivées. La détection et la télémétrie par la lumière utilisent la lumière ultraviolette, visible ou proche de l'infrarouge pour représenter les objets captés et peuvent être utilisées pour détecter une large gamme d'objets, y compris les objets non métalliques, les roches, la pluie, les composés chimiques, les aérosols, les nuages, les molécules individuelles et même les déplacements souterrains.

91 À la différence de la violence physique, aucune institution ou individu ne peut prétendre au monopole de la violence symbolique, puisque des institutions privées peuvent également l'exercer (famille, sectes, etc.).

92 Jett Jennifer, « China's new map outrages its neighbors », NBC News, 1er septembre 2023.

production de données géographiques est également un levier de légitimation du contrôle de l'État sur son territoire dédié aux puissances étrangères qui chercheraient à remettre en doute sa souveraineté.

La souveraineté est un principe fondamental du droit international. Son origine latine, *sui juris*[93], *esse suae potestatis*[94], ou *summa potestas*[95], indique que la souveraineté fait référence à l'autorité suprême du prince ou du roi ou appliquée au droit international moderne, de l'État. Une définition largement acceptée de la « souveraineté » a été énoncée par la sentence arbitrale de l'île de Palmas en 1928. Elle prévoit que : *« la souveraineté dans les rapports entre États signifie l'indépendance. L'indépendance en ce qui concerne une partie du globe est le droit d'y exercer, à l'exclusion de tout autre État, la fonction d'État »*[96].

La souveraineté nationale procède également de la volonté commune d'un peuple pour faire nation sur un territoire commun. De cette volonté commune, elle retire puissance et légitimité politique. L'État souverain est ainsi une collectivité humaine stabilisée sur un territoire, au sein de laquelle la contrainte est légitimement monopolisée. La souveraineté d'un État se fonde donc sur l'approbation de sa population et la reconnaissance par cette dernière de sa légitimité, en même temps qu'elle s'exerce sur cette même population. Elle s'applique sur l'intégralité du territoire de cet État, mais aussi, par extension, sur son espace maritime (par ex., la zone économique exclusive de 200 milles marins des côtes), sur un espace aérien (plus difficilement définissable puisqu'il est compris comme l'espace sub-atmosphérique avec plusieurs « couches » différenciées » et sur le sous-sol de ce même territoire. Pour être effective et non uniquement un principe juridique, la souveraineté doit aller de pair avec la préservation de la puissance de l'État souverain, compris ici comme sa capacité à agir de façon autonome.

Le principe de souveraineté, reconnu dans le droit international, s'applique également à l'ensemble des infrastructures numériques. Comme le souligne le désormais célèbre manuel de Tallinn sur les opérations dans l'espace cyber, les États jouissent de la souveraineté sur toute infrastructure numérique située sur leur territoire et sur les activités associées à cette infrastructure[97]. Bien que la territorialité soit au cœur du principe de souveraineté, dans certaines circonstances, les États peuvent également exercer des prérogatives souveraines, telles que la juridiction sur les cyber-infrastructures et les activités à l'étranger, ainsi que sur certaines personnes engagées dans ces activités. Enfin, la nature territoriale de la souveraineté impose également des restrictions aux cyber-opérations d'autres États

---

93 En latin : Son droit propre.

94 En latin : Être en son pouvoir.

95 En latin : La puissance la plus élevée

96 Cour permanente d'Arbitrage, « Sentence arbitrale rendue le 4 avril 1928, par M. Max Huber, entre les États-Unis et les Pays-Bas, dans le litige relatif à la souveraineté sur l'île de Palmas (ou Miangas) », traduit par M. Ch. Rousseau, in *Revue générale de Droit international public,* p. 156, 1935.

97 Schmitt Michael N. et Vihul Liis (dir), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

visant des infrastructures numériques situées sur le territoire souverain dudit État. Les couches physique, logique et sociale du cyberespace sont englobées dans le principe de souveraineté. Le Manuel 2.0 de Tallinn souligne ainsi que les activités au sein du cyberespace *« se déroulent sur un territoire et concernent des objets, ou sont menées par des personnes ou des entités, sur lesquelles les États peuvent exercer leurs prérogatives souveraines »*[98]. Bien que les cyber-activistes puissent franchir de multiples frontières, ou se dérouler dans les eaux internationales, l'espace aérien international ou l'espace extra-atmosphérique, toutes sont menées par des personnes ou des entités soumises à la juridiction d'un ou de plusieurs États. Le fait qu'une infrastructure numérique située sur le territoire d'un État donné soit liée au cyberespace ne peut être interprété comme un renoncement à sa souveraineté. En effet, les États ont le droit, en vertu du principe de souveraineté, de déconnecter de l'Internet, en tout ou en partie, toute infrastructure numérique située sur leur territoire, sous réserve de toute restriction conventionnelle ou de droit international[99].

Aujourd'hui omniprésent, et souvent utilisé de façon floue, le terme de cyberespace nécessite d'être précisément défini dans la présente étude. Le cyberespace ou espace numérique désigne l'ensemble des équipements informatiques du monde et de leurs différentes formes de mise en réseau. L'espace numérique est constitué de quatre couches. La couche matérielle rassemble l'ensemble des appareils, serveurs, routeurs, ordinateurs qui permettent l'interconnexion des machines. Ainsi, le cyberespace est loin d'être aussi immatériel qu'on se le figure souvent. Le cyberespace s'appuie sur un ensemble d'infrastructures à la réalité physique indéniable et à la position géographique précise, des plus petits serveurs en passant par les immenses câbles sous-marins. La multiplication des appareils de connexion à distance (4G, Wifi, Bluetooth…) renforce le sentiment de virtualité du cyberespace parmi les utilisateurs (ou consommateurs) du cyberespace, mais il s'agit bien là d'un espace physique comme le souligne Olivier Kempf (2012)[100]. La couche logique est constituée des connexions qui existent entre les périphériques du réseau. Elle comprend les applications, les données et les protocoles qui permettent l'échange de données à travers la couche physique. C'est cette couche qui permet de passer du langage informatique au langage humain. L'ensemble des langages de programmation et des protocoles qui régissent les interactions entre machines sont compris dans cette couche. Aujourd'hui le protocole d'échange le plus répandu est le modèle TCP/IP (Transmission Control Protocol/ Internet Protocol)[101], que l'on décrit souvent par comparaison avec le modèle OSI (cf. Figure 1).

---

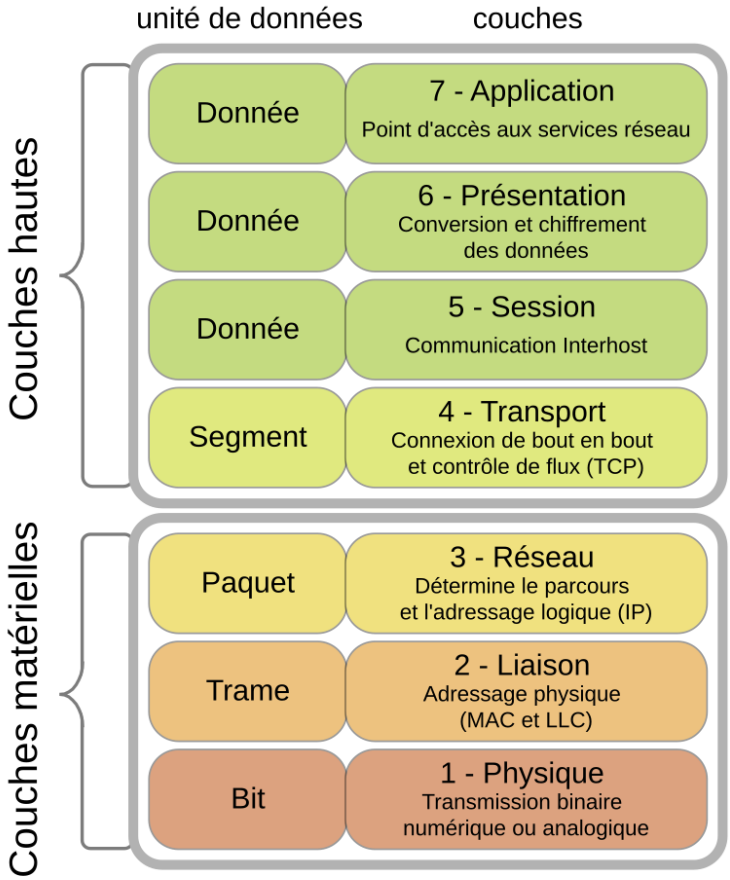
98 Ibid.

99 Schmitt Michael N. et Vihul Liis (dir), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, op. Cit., commentaire de la règle 1, paragraphe 1 et paragraphe 10.

100 Kempf Olivier, « Introduction à la cyberstratégie », Paris, Economica, p. 76, 2012.

101 Stevens W. R., « TCP/IP Illustrated : The Protocols », AddisonWesley Professional, 1994.

Figure 1 : Diagramme du modèle OSI



Source : *Fortinet (2015)*

Il est intéressant de noter que, si le modèle TCP/IP est né au sein des laboratoires de la DARPA et a constitué la fondation du modèle d'échange de donnée d'ARPANET (ancêtre d'Internet), le modèle TCP/IP ne s'est pas imposé comme une norme *de jure* sanctionnée par une organisation internationale. C'est la compétition féroce entre les différents géants des technologies de la communication de l'époque, au premier rang desquels se trouvaient Lucent, Nortel ou encore Cisco[102], et la victoire sur le marché du modèle défendu par Cisco et Nortel qui a fait émerger le modèle TCP/IP, comme le protocole privilégie des échanges internationaux sur Internet et norme *de facto*, aux dépens d'autres modèles, comme l'ATM (Asynchronous Transfer Mode) défendu par Lucent jusqu'en 1999[103]. En effet,

[102] On pourrait également citer dans cette liste d'autres sociétés, telles que : Fujitsu, NEC, GEC (Marconi), Siemens, Nokia, Motorola, Tellabs, ou encore Ciena.

[103] Lazonick William et March Edward, « The rise and demise of Lucent Technologies », University of Massachusetts, Dartmouth College, 2010.

entre 1998 et 2000, la société Lucent, alors leader sur le marché des réseaux de données, a investi massivement dans le rachat de sociétés proposant des réseaux fondés sur le modèle ATM. Ce modèle était alors conçu comme un concurrent au modèle de transfert de données TCP/IP défendu par Nortel et Cisco. Cependant, dès 1999 Lucent abandonne sa stratégie d'investissement dans le modèle ATM, reconnaissant par là son échec retentissant à en faire un concurrent viable au modèle TCP/IP. Ce dernier devient le standard *de facto* dominant pour tous les échanges de données sur Internet.

Le cyberespace est également composé d'une couche sémantique ou informationnelle qui correspond à l'ensemble des informations qui transitent dans le cyberespace. La notion d'information est polysémique et peut désigner à la fois des informations informatiques qui permettent aux réseaux informatiques de communiquer, ou tout autre type d'informations, comme les informations médiatiques ou de renseignement. L'information diffusée au sein du cyberespace est une partie pleine et entière du cyberespace lui-même et participe à modeler ce dernier autant qu'elle est modelée par lui, en fonction des modalités de diffusion de ces informations. Ainsi, la couche sémantique du cyberespace occupe une place centrale dans la façon dont les États vont interagir avec ce dernier. Si certains pays vont se pencher très fortement sur les contenus disponibles au sein du cyberespace parcouru par leurs utilisateurs nationaux (Russie et Chine en tête), d'autres États, notamment en Occident, ont une approche plus libérale des informations diffusées sur le cyberespace. Cependant, même dans les régimes libéraux, le contrôle des informations diffusées, nécessaires au respect de la loi, en particulier concernant la diffusion de messages de haine ou appelant à la violence contre certains groupes d'individus, reste nécessaire. Là encore, contrairement à une idée reçue, le cyberespace est loin d'être ce « Far West » où tout est permis, et fait l'objet depuis ses débuts, et de plus en plus, d'une surveillance plus ou moins accrue de tous les États qu'il recouvre. Enfin il existe une quatrième couche, la couche sociale, qui englobe les individus et les groupes engagés dans des activités dans le cyberespace. L'ensemble de ces couches doivent communiquer entre elles et l'Internet mondial s'appuie sur un large ensemble de normes pour pouvoir permettre l'interconnexion des matériels et des humains au sein du cyberespace.

Le cyberespace est donc à la fois physique et abstrait et présente pour celui qui cherche à en faire l'analyse l'image d'un espace dual à la fois composé d'éléments tangibles (l'infrastructure informatique) et intangibles (les données, représentations et interactions générées par ses utilisateurs). En cela le cyberespace est un espace complexe, étant à la fois un espace individuel, lui-même composé de multiples « lieux » générés par l'ensemble des interactions de ses utilisateurs. La notion d'espace est à prendre ici au sens le plus large de lieu plus ou moins délimité où se situe quelque chose. Le cyberespace considéré dans sa globalité, de par sa nature interconnectée, correspond à cette définition en délimitant un seul et même espace global qui s'étend aujourd'hui sur toute la planète. Cependant,

l'interconnexion du cyberespace n'est pas totale. Certains lieux du cyberespace sont a accès restreint, comme l'Internet chinois protégé par la grande muraille de Chine numérique érigé par la RPC. Le cyberespace est donc également divisé en différents lieux plus ou moins ouverts, qui peuvent interagir ou fonctionner en vase clos. Ces lieux sont à la fois matériels et immatériels réparties en des milliers de lieux sur l'ensemble du globe. Le fait que le cyberespace soit bien un espace en fait par la même occasion une composante de la stratégie internationale de chaque État, en ce qu'il un « espace dans l'espace » de l'État au sein duquel va pouvoir se déployer différentes stratégies propres à garantir la souveraineté de l'État dans sa parcelle de cyberespace, en ce qu'il constitue un espace, au même titre que son territoire physique, sur lequel s'exerce sa souveraineté. Comme le soulignait Raymond Aron (1967)[104], la prise en compte de l'espace est un élément indispensable à toute étude des relations internationales et constitue à la fois le milieu sur lequel s'exprime ces relations et un enjeu de ces mêmes relations. À ce titre le cyberespace constitue depuis sa création un des milieux de la compétition internationale. Le cyberespace, au même titre que l'espace géographique, est donc une composante essentielle de la préservation de la souveraineté d'un État moderne.

Ainsi, la normalisation, et à fortiori celle des données géographiques numériques, implique des enjeux de souveraineté en ce qu'elle a une influence certaine sur la façon dont les États produisent et diffusent un savoir qui touche à une de leur prérogative régalienne qui est la délimitation et la défense de leur territoire. Le caractère numérique des données géographiques qui les place dans le champ du cyberespace dès qu'elles sont produites et diffusées renforce également cet enjeu de souveraineté aux yeux des États qui les produisent, puisque ces derniers ont la responsabilité de surveiller les informations diffusées dans le cyberespace au sein de leur territoire et ont un intérêt important à protéger et préserver les informations géographiques qu'ils souhaitent voir diffuser au sein du cyberespace. Le rôle de la normalisation pour remplir cette mission est ici double. Non seulement le processus normatif est la condition sine qua non d'une production et d'une diffusion efficace de ces données, mais il permet également, comme il sera démontré plus loin, de fluidifier la diffusion de mesure de protection contre des attaques cyberpotentielles contre ces mêmes données, en intégrant dans le processus de conception de ces données ou dans leurs règles d'implémentation des mesures de sécurité.

[104] Aron Raymond, « Qu'est-ce qu'une théorie des relations internationales ? », *Revue française de science politique*, n° 5, 1967, p. 837 – 861.

1.2 Histoire de la normalisation internationale

Le processus historique et politique par lequel les différents pays ont été amenés à structurer leurs organismes de normalisation nationaux reste tout sauf normalisé. De grandes différences existent entre les différents pays qui composent la scène de la normalisation internationale, et cela tient pour une bonne partie à leur histoire. Ainsi, au cours de la première moitié du vingtième siècle, les approches nationales en matière de normes se sont cristallisées en fonction de leurs origines chronologiques, juridiques et sociopolitiques respectives[105]. La littérature consacrée à l'économie de la normalisation, et en particulier les travaux de Greenstein (1992)[106], a mis en évidence le fait que tous les systèmes de normalisation nationaux reposent sur un agencement de trois composantes fondamentales, à savoir la concurrence entre acteurs privés, la coopération volontaire entre parties prenantes et la coercition exercée par la puissance publique. La façon dont ces trois composantes se combinent varie considérablement d'un pays à l'autre et a évolué au fil du temps, la tendance générale étant néanmoins celle d'un recul progressif de l'intervention étatique directe au profit d'un modèle de développement plus libéral faisant la part belle aux acteurs privés.

Les pays ayant adopté des normes nationales en premier l'ont fait sous l'impulsion de coalitions d'acteurs privés, qui ont favorisé très tôt des approches fondées sur le libre marché et la concurrence. L'Allemagne est ici un bon exemple. Le NDI (Normenausschuss der Deutschen Industrie, Comité allemand de normalisation industrielle), fondé en 1917, ne rassemblait à l'origine que des groupes industriels. Aujourd'hui appelé DIN (Deutsches Institut für Normung e.V., Institut allemand de normalisation), il est resté un organisme entièrement privé jusqu'en 1975, date à laquelle il est devenu l'organisme de normalisation nationale en République fédérale d'Allemagne (RFA). D'autres pays, qui se sont industrialisés plus tardivement, se sont appuyés sur les exemples donnés par les pays les plus précoces, et notamment sur les déséquilibres entraînés par une approche purement libérale, pour développer des approches plus équilibrées mêlant dirigisme et libéralisme. Enfin, les pays les plus en retard technologiquement, qui ont vu leurs organes nationaux de normalisation être créés dans la seconde moitié du XXe siècle, ont eu tendance à s'appuyer davantage sur la contrainte directe de l'État[107]. Ce phénomène rejoint l'analyse plus générale proposée par Gerschenkron (1962) sur le rattrapage économique des pays tardivement industrialisés, selon laquelle l'absence d'une classe entrepreneuriale suffisamment structurée conduit l'État à jouer un rôle moteur dans l'organisation de

---

105 Carl F. Cargill, « Information Technology Standardization: Theory, Process and Organizations », Bedford : Massachusetts, Digital Equipment Corporation, 1er janvier 1989.

106 Shane M. Greenstein, « Invisible Hands and Visible Advisors: An Economic Interpretation of Standardization. », *Journal of the American Society for Information Science*, n° 43, septembre 1992.

107 Gerschenkron Alexander, « Economic Backwardness in Historical Perspective », Cambridge : Massachusetts, Harvard University Press, 1962.

l'économie. En matière de normalisation, cette logique se vérifie pleinement : de nombreux pays capitalistes d'Asie de l'Est, comme la République populaire de Chine et le Japon, ont des institutions de normalisation presque entièrement gérées par l'État, alors qu'en Europe occidentale, seul le Portugal est dans ce cas.

La politique a également grandement influencé la construction des différents modèles d'organisation de la normalisation au sein des différents pays. En effet, les approches nationales en matière de normalisation ont eu tendance à se former au cours de la période, généralement la première moitié du XXe siècle, pendant laquelle les institutions nationales de normalisation ont été créées pour la première fois. Comme l'a montré Haber (1991) dans son étude des professions américaines[108], dans les pays où les professions occupées par la classe moyenne étaient dominantes avant l'industrialisation, les professions libérales préindustrielles sont devenues le modèle qui a structuré plus tard l'ingénierie et d'autres professions techniques, soutenant ainsi une approche durablement libérale des normes. La Grande-Bretagne, la France et les États-Unis étaient des pays de ce type, bien que l'implantation libérale ait été plus faible en France, où le modèle antilibéral du régime de Vichy a eu des effets qui ont duré longtemps après l'occupation, comme nous le verrons plus loin. Cependant, comme l'a souligné Luebbert (1991)[109], dans les pays où l'élaboration initiale des institutions nationales de normalisation s'est déroulée sous des régimes politiques antilibéraux, les marchés libres et les professions libérales ont été rejetés en faveur d'une subordination politique des marchés. De fait, partout où l'hégémonie des entreprises privées a été sérieusement remise en question, que ce soit par la droite ou par la gauche, une approche plus coordonnée des normes a vu le jour et a eu tendance à persister.

De plus, non content de devenir un élément central de la stratégie des entreprises, les différences nationales en matière de normalisation ont également des implications importantes pour tout ce qui concerne la protection de la vie privée et le comportement des consommateurs, les modèles de construction nationale, les relations internationales et les mouvements sociaux mondiaux. Une meilleure compréhension des approches nationales en matière de normalisation est essentielle pour mieux comprendre les dynamiques de pouvoir entre les différents acteurs nationaux et internationaux qui participent à la normalisation internationale. Dans ce contexte il est intéressant de se pencher sur le cas de la France, qui est non seulement au cœur de la présente étude, mais qui comporte également certaines caractéristiques historiques et culturelles qui la distinguent de la majorité des pays occidentaux en matière de conception de normes.

---

[108] Haber Samuel, « The Quest for Authority and Honor in the American Professions, 1750-1900 ». Chicago, University of Chicago Press, 1991.

[109] Luebbert Gregory M., « Liberalism, Fascism, or Social Democracy: Social Classes and the Political Origins of Regimes in Interwar Europe », New York, Oxford University Press, 25 juillet 1991.

1.2.1 Le cas de la France

Comme l'a analysé Tate (2011)[110], la France constitue un cas singulier dans l'histoire de la normalisation, en ce que le choix d'une approche libérale ou coordonnée a profondément divisé les entreprises françaises dès la Révolution française. Bien que la nature de ce clivage ait changé avec le temps, sa persistance a conduit à l'utilisation récurrente de ce que Burrin a qualifié de *« libéralisme sous surveillance »*[111], qu'il soit gaulliste ou bonapartiste, dans lequel les entreprises acceptent la présence d'intermédiaires désignés par l'État plutôt que de poursuivre des stratégies entièrement libérales ou entièrement coordonnées. Ainsi, en France, les corporations industrielles, illégales depuis la loi Le Chapelier de 1791[112], ont été confrontées à des conditions particulièrement difficiles. Alors que l'Allemagne optait pour une coordination accrue du secteur privé à la fin de la Première Guerre mondiale, la France a choisi une voie différente en créant un organisme public de normalisation, la Commission permanente de Normalisation (CPN), en 1918. La première norme de la CPN a été publiée en 1920, mais le manque de soutien de la part des industriels pour cette structure a mené à sa fermeture en 1924. Ces derniers critiquant son caractère trop centralisateur et étatique[113]. En 1926, les entreprises françaises ont alors créé leur propre organisme national privé de normalisation, l'Association française de Normalisation (AFNOR), toujours en activité aujourd'hui.

En août 1940, alors que les régions du nord de la France sont directement occupées, le patronat français organise à Paris des comités d'organisation sectoriels (COS) investis de pouvoirs publics leur permettant d'imposer des cotisations et de proposer des sanctions. Pendant la période de guerre, où l'obtention de matériaux et la simple survie étaient devenues de plus en plus difficiles, le gouvernement de Vichy est intervenu avec le soutien d'entreprises, telles que Peugeot[114]. Le décret de normalisation du 24 mai 1941, confirmé par une ordonnance de 1944, a permis au gouvernement de Vichy de réglementer la normalisation, pour contrer la domination allemande sur les entreprises françaises de la zone occupée. Un commissaire général à la normalisation a été nommé pour superviser la relation entre la normalisation privée et l'État. L'État était chargé d'approuver l'ouverture ou la fermeture de tout projet de normalisation, la nomination de tout le personnel clé et même la programmation des réunions[115]. L'approche de Vichy en matière de normes a perduré près de quatre décennies après la

---

110 Tate Jay, « National Varieties of Standardization », in Hall Peter A. et Soskice David (dir)., Varities of Capitalism : The Institunal Foundations of Comparative Advantage, Oxford, Oxford University Press, 2011, pp. 442 – 473.

111 Burrin Philippe, « La France à l'heure allemande (1940-1944) », Paris, Seuil, p. 321, 1995.

112 Promulguée en France le 14 juin 1791, la loi dite Le Chapelier est une loi ayant interdit tout groupement professionnel, qu'il s'agisse des guildes ou des corporations. Elle se concentre en particulier sur les organisations ouvrières et interdit de fait les syndicats ouvriers.

113 Jones Adrian, « Illusions of Sovereignty: Business and Organization of Committees of Vichy France. », in *Social History*, n° 11, 1er janvier 1986.

114 Vinen Richard, « Politics of French Business, 1936-1945. », New York, Cambridge University Press, 1991.

115 *Ibid*

Libération. Même après la guerre, les entreprises françaises appréciaient la coordination technocratique, qui leur permettait de chercher ouvertement des soutiens au sein de la classe politique. La coalition à l'origine de la norme française alternative pour la télévision couleur (SECAM : Séquentielle Couleur à Mémoire) en 1960 est peut-être l'exemple le plus connu[116]. Inventé en 1956 par l'ingénieur français Henri de France, le Sécam est une norme internationale de codage couleur du signal vidéo analogique. Ce format est adopté en France en 1960 et est fortement soutenu par les autorités françaises de l'époque, pour être adopté comme norme internationale de codage en Europe. Ainsi, en 1966, lors de la conférence annuelle de l'Union Internationale des télécommunications (UIT) d'Oslo, le Sécam est en concurrence avec la norme PAL (phase Alternating Line ou ligne alternante la phase en Français) de la société allemande Telefunken. L'enjeu devient très vite politique et entraîne l'intervention du président Charles de Gaulle et du Premier ministre Georges Pompidou pour soutenir le Sécam. Finalement les deux normes seront autorisées en Europe à l'exclusion de toutes les autres. Cependant le Sécam ne rencontrera que peu de succès en Europe. Avec l'émergence des téléviseurs bistandards PAL-SECAM dans les années 1970, la plupart des pays abandonnent le Sécam, à l'exclusion de la Russie et de la Biélorussie. Le Sécam s'exportera cependant en Afrique, notamment dans les anciennes colonies françaises et belges. La célèbre norme « Label rouge » pour les produits agricoles de haute qualité, créée en 1960 par le ministère de l'Agriculture, est un autre exemple de normalisation dirigiste, dans un secteur différent.

Il faut attendre 1981 et l'arrivée au pouvoir d'un gouvernement socialiste, pour que le système mis en place sous Vichy commence à être remis en cause. Une grande partie de la supervision de la normalisation par l'État est alors transférée à l'AFNOR en 1984, et le commissaire à la normalisation créé par Vichy a arrêté de publier de nouvelles normes « enregistrées ». La réglementation nationale détaillée des normes a été remplacée par une « nouvelle approche » donnant plus de pouvoir à l'AFNOR. Les entreprises françaises ont également soutenu une « nouvelle approche » comparable au niveau européen[117]. En 1992, le Conseil supérieur de la normalisation a été supprimé et ses fonctions ont été transférées à l'AFNOR (cf. Figure 2). La part de l'élaboration des normes AFNOR confiée aux bureaux de normalisation externes est passée d'un tiers en 1980 à la moitié dans les années 1990. Malgré l'adoption de cette « nouvelle approche », la majorité des entreprises françaises impliquées dans la normalisation à l'époque la considère comme une charge et une contrainte[118]. Toutefois, elles continuent de participer en raison des subventions de l'État qui les y incitent. En 1992, des déductions fiscales ont été mises en place pour encourager les dépenses liées à la participation à la normalisation

[116] Crane Rhonda J., « The Politics of International Standard Setting: France and the Color TV War. », Norwood, 1979.
[117] Site Internet France normalisation au sujet de la nouvelle approche : https://www.francenormalisation.fr/les-acteurs-de-la-normalisation/la-nouvelle-approche/
[118] Duffaux Karine, « La Démarche productive : une approche en termes d'héritage, la perspective allemande. », 1995.

de l'AFNOR, entraînant une augmentation soudaine du nombre de participants à la normalisation française, qui ont atteint des niveaux comparables ceux observés en Allemagne. Aujourd'hui, le décret n °2021-1473 du 10 novembre 2021, modifiant le décret n °2009-697 du 16 juin 2009, définit les cadres du système de normalisation français, en établissant les principes essentiels de la politique de normalisation nationale et le rôle de ses différents acteurs.

Figure 2 : La normalisation internationale en France et dans le monde

1901	Création de la première organisation de normalisation au Royaume-Uni, l'« Engineering Standard Committee »
1906	Création de la Commission Internationale pour l'électrotechnique
1918	Création en France de la Commission Permanente de Normalisation (CPN)
1926	Fondation de l'Association française de normalisation (AFNOR)
1941	Le gouvernement de Vichy créé le Commissariat Général à la Normalisation
1946 - 1947	Fondation de l'Organisation Internationale de Normalisation (ISO)
1961	Création du Comité Européen de Normalisation (CEN)
1984 - 1992	Abolition du Commissariat Général à la Normalisation au profit de l'AFNOR
1994	Création du Comité Technique de l'ISO sur les informations géographiques, ainsi que de l'Open Geospatial Consortium (OGC)

Source : *AFNOR (2025)*

Les entreprises françaises ont donc été confrontées historiquement à un environnement normatif hétérogène et en constante évolution. Pour reprendre la typologie proposée par Tate[119], le modèle

[119] Tate Jay, « National Varieties of Standardization », in Hall Peter A. et Soskice David (dir)., Varities of Capitalism : The Institunal Foundations of Comparative Advantage, Oxford, Oxford University Press, 2011, pp. 442 – 473.

français se distingue à la fois des approches libérales, fondées sur la concurrence de marché, et des approches coordonnées, fondées sur la coopération interentreprises, en ce que la médiation stratégique par l'État y occupe une place structurante qui n'a pas d'équivalent parmi les grandes nations industrialisées occidentales. En conséquence, elles sont particulièrement présentes dans les secteurs où ce type de médiation est le plus prononcé, comme dans les domaines des produits de luxe ou encore les transports et les communications, largement soutenus par l'État. En fonction des acteurs concernés et des avantages qu'ils pensent pouvoir en retirer, les incitations à la normalisation sont mixtes, souvent élevées à la fois pour participer ou ne pas le faire. Les professionnels tiers, tant à l'intérieur qu'à l'extérieur de l'État (les autorités régionales ajoutent un facteur supplémentaire), génèrent des pressions exogènes, en faveur de la normalisation. Mais la médiation de l'État attire également les entreprises à la recherche d'une protection commerciale fondée sur des normes soutenues politiquement, et d'autres avantages tactiques. Aujourd'hui l'État, par le biais de l'AFNOR, incite fortement les industries françaises à participer aux efforts de normalisation internationaux, et ce, dans tous les secteurs industriels.

Cependant, si la France occupe une place importante au sein d'organismes de normalisation, comme au sein de l'organisation internationale de normalisation, du fait du développement assez chaotique de la normalisation au sein des industries françaises jusque dans les années 1990, elle reste en retrait par rapport à des pays comme l'Allemagne. En effet, ces derniers ont très tôt vu leur secteur industriel corporatiste se coaliser au sein de ses différents secteurs afin de mieux peser dans les discussions internationales relatives à la normalisation, dès la première moitié du vingtième siècle.

Si aujourd'hui la France présente un environnement normatif plus classique et orienté vers le volontarisme des entreprises privées, il présente également un aspect très stratifié entre les différents acteurs français de ce système normatif qu'il est important d'analyser afin de saisir comment ce dernier fonctionne.

1.3 Le système français de normalisation

Dans son rapport remis en décembre 2014 au ministre de l'Économie, de l'Industrie et du Numérique, Lydie Evrard, alors déléguée interministérielle aux normes, définit le système français de normalisation comme :

> *« l'ensemble des acteurs et des organisations destinés à assurer que le processus de normalisation est mené selon les objectifs fixés par le décret du décret 16 juin 2009, qui définit la normalisation comme une activité d'intérêt général ayant pour objet de fournir des documents de référence, élaborés de manière consensuelle par toutes les parties intéressées, afin d'encourager le développement économique et l'innovation, tout en prenant en compte les objectifs de développement durable »*[120].

Le système français de normalisation regroupe de très nombreux acteurs, issus à la fois des institutions publiques, des sociétés privées, mais concerne également les consommateurs, représentés par le biais d'associations en charge de veiller à la prise en compte de leurs besoins. Dans l'idéal tous ces acteurs se doivent d'être correctement représentés et écoutés. Les travaux de normalisation se doivent également d'être menés de façon transparente afin que l'ensemble des partis prenant puissent être dûment informés des avancées dans ce domaine. Enfin, la dimension internationale dans laquelle s'inscrit le système français est un élément crucial dans l'analyse de son fonctionnement et du rôle joué par ses différents acteurs. Les textes officiels ne donnent pas de définition précise du terme de « système français de normalisation », bien qu'il soit régulièrement employé dans la littérature. Le système français de normalisation apparaît dans le titre du premier chapitre du décret du 10 novembre 2021. Plusieurs acteurs institutionnels sont absents de la définition qui y est donnée, tels que les responsables interministériels aux normes. Cette situation est un bon exemple du flou institutionnel qui persiste encore aujourd'hui quant au rôle de l'ensemble des acteurs de la normalisation française, qui, si on se rapporte à la définition donnée par Lydie Evrard, doit être élargie par rapport à ce qui est indiqué dans le décret du 10 novembre 2021. Dans tous les cas, il est nécessaire de reprendre l'ensemble des acteurs concernés et leur rôle afin de dresser le panorama du système français de normalisation.

En France, l'activité de normalisation est menée par la collaboration de l'ensemble des parties prenantes au sein de deux catégories d'instances distinctes. D'une part, il existe des instances dotées d'une mission stratégique en vue de contribuer au pilotage ou à la coordination de la stratégie française en matière de normalisation, et, d'autre part, il y a des instances qui se concentrent sur la définition du contenu des normes ou des positions à promouvoir au sein des organes de normalisation européens ou internationaux.

L'AFNOR constitue de loin l'acteur principal de ce système, jouant à la fois un rôle stratégique et contribuant à l'élaboration des normes. Fondé en 1926, le groupe AFNOR est une organisation internationale, chargé d'une mission d'intérêt général et qui exerce une activité marchande. En 2022, le

[120] Evrard Lydie, « Politique nationale de normalisation et stratégie pour la compétitivité de notre économie », Rapport remis au ministre de l'Économie, de l'industrie et du numérique, p. 3, décembre 2014.

groupe AFNOR comptait 1 490 membres adhérents, dont 86 % d'entreprises et 1 210 salariés. Son chiffre d'affaires s'élève à 188,8 M€, dont 6,1 M€ de subventions publiques, pour un bénéfice net de 5 M€[121]. Même si l'AFNOR est reconnue d'utilité publique et investie d'une mission de service public, il ne s'agit pas d'une émanation directe de l'État. En effet, la confusion entre le rôle de l'État et celui du groupe AFNOR est fréquente, mais l'AFNOR reste un groupe aux intérêts propres et ne dépend pas entièrement de l'État pour ses revenus. L'intervention de l'État, en tant que responsable de la politique de normalisation, s'exprime principalement à travers un contrat pluriannuel d'objectifs conclu avec l'AFNOR, ainsi que par le rôle du Commissaire du Gouvernement confié au délégué interministériel aux normes, conformément au décret du 10 novembre 2021. La production de norme en France est donc soumise en partie aux impératifs de l'AFNOR qui se doit de trouver ses propres voies de financement, parmi lesquels la vente de norme tient une place importante. Ainsi, en 2022, les revenus du groupe AFNOR provenaient principalement de leur activité de certification auprès des entreprises (55 %), de la vente de leur travail d'édition de normes (20 %), de la vente de normes (16 %) et de leur offre de formation (9 %)[122]. Le monopole de l'AFNOR sur le développement et la mise à disposition de normes internationales est régulièrement débattu comme un des plus grands freins à la diffusion des normes en France. Et, par extension, à la connaissance des travaux de normalisation par l'ensemble des acteurs concernés par leur production. En effet, si les normes rendues obligatoires par des lois ou décrets sont mises à disposition gratuitement par l'AFNOR, ces dernières représentent moins de 1 % des normes disponible s[123]. Le caractère restrictif donné à la définition de normes obligatoire aboutit régulièrement à des situations ubuesques où des corps de métiers se retrouvent à payer plusieurs centaines d'euros en moyenne pour avoir accès à des normes de facto obligatoires à l'exercice de leur métier. Ainsi, la norme utilisée par tous les chercheurs et bibliothécaires pour citer une publication et rédiger une bibliographie[124], qui était anciennement la norme française Z44-005[125], n'est pas consultable gratuitement. Elle coûte 209,34€ hors taxe s[126]. Il est important de noter que, comme l'indique Barthe (2021), *« ce sont les bibliothécaires, agissant notamment à travers leurs fédérations*

[121] Groupe AFNOR, « Rapport d'activité et de responsabilité sociétale 2022 », 2023.

[122] *Ibid*.

[123] Avec 501 normes obligatoires sur un total d'environ 37 500 en 2023 selon les données de l'AFNOR, la proportion représente effectivement plus de 1 %. Cependant, il est crucial de noter que l'AFNOR a exclu de cette liste les normes élaborées par des organismes européens et internationaux, qui détiennent des droits de propriété intellectuelle sur celles-ci. Par conséquent, en prenant en compte cette exclusion, on se retrouve en réalité avec une proportion inférieure à 1 %.

[124] NF ISO 690, « Information et documentation - Principes directeurs pour la rédaction des références bibliographiques et des citations des ressources d'information », août 2010.

[125] https://fr.wikipedia.org/wiki/NF_Z_44-005

[126] https://m.boutique.afnor.org/fr-fr/norme/nf-iso-690/information-et-documentation-principes-directeurs-pour-la-redaction-des-ref/fa153497/1090

professionnelles et institutions nationales, qui assument le rôle d'auteurs et de traducteurs de ces normes. Ni l'AFNOR ni l'ISO ne sont les instigateurs de ces travaux »[127].

La position de monopole de l'AFNOR, qui est lié à la fois à son ancienneté et au réseau d'experts qu'elle fédère, est également un impératif qui permet d'assurer que deux projets de normes contradictoires ne se développent pas au même moment. Cette situation de monopole de la part de l'organisation nationale de normalisation, qu'elle soit publique ou privée, comme l'AFNOR, se retrouve dans tous les pays impliqués dans la normalisation internationale et concerne toutes les échelles territoriales. Ainsi, à l'échelle européenne, seule l'AFNOR est habilitée à représenter les intérêts français au sein du CEN et du CENELEC. L'AFNOR occupe donc également une position de lobby des normes qui a à cœur de défendre ses propres intérêts. Le résultat de ce lobbying se retrouve dans la conception du décret n °2009-697 du 16 juin 2009, modifié par le décret n °2021-1473 du 10 novembre 2021, qui avait été annoncé comme devant amorcer une plus grande gratuité des normes, il n'en a rien été[128]. De nouveau, en 2016, lors du vote de la loi pour une République numérique, l'AFNOR a obtenu que les normes soient exclues du champ de l'open data et restent par conséquent soumises au droit d'auteur et payantes[129]. L'argument avancé pour justifier cela était que l'AFNOR étant en charge de représenter la France à l'international, elle était obligée de se soumettre aux règlements de l'ISO/IEC et du CEN/CENELEC qui interdisent de diffuser les normes gratuitement. Le fait est que l'AFNOR reste extrêmement attachée à la manne financière que représente la vente de norme, car, même si le groupe se targue de résultats financiers positifs dans ses rapports annuels, la part du soutien de l'État dans son chiffre d'affaires ne cesse de baisser depuis 2010. Alors que la subvention de l'État s'élevait à 14M€ entre 2006 et 2010, cette dernière est en baisse significative chaque année depuis lors, atteignant en 2023 seulement 6,3M€[130]. Inciter les acteurs privés à investir dans des projets de normalisation et maintenir des frais de participations aux comités techniques de normalisation représentent donc toujours des enjeux cruciaux pour l'AFNOR, quand bien même cela constitue un frein significatif à la participation de certains acteurs de la société civile. Aujourd'hui la vente de norme elle-même ne représente plus que 16 % du chiffre d'affaires de l'AFNOR, largement dépassée par la vente de certification (55 %). Cela démontre un changement de paradigme dans le monde de la normalisation, où les normes sont de plus en plus perçues par les acteurs économiques comme des moyens détournés de sponsoriser leur activité, en apposant une marque reconnaissable par leurs clients sur leurs produits, pour s'en servir comme levier pour gagner des parts de marché. Un grand nombre de

127 Barthe Emmanuel, « Les normes, l'AFNOR et leur financement – Ou pourquoi les normes ne sont pas près de devenir gratuites », novembre 2021.
128 Barthe Emmanuel, « Vers une privatisation des normes ? », décembre 2009.
129 Champeau Guillaume, « Le Sénat exclut les normes AFNOR de l'Open Data », Numerama, 27 avril 2016.
130 Groupe AFNOR, « Rapport d'activité et de responsabilité sociétale 2022 », 2023.

TPE et de PME observent le développement de normes de façon attentiste, sans y participer activement, préférant préserver leurs économies pour obtenir une certification AFNOR une fois les nouvelles normes disponibles sur le marché. Cette mentalité n'encourage pas un grand nombre de sociétés à participer activement aux travaux de normalisation et ne participe pas à augmenter le poids de la France sur la scène internationale de la normalisation. Il apparaît donc qu'il sera nécessaire à plus ou moins long terme de voir augmenter le soutien financier à l'AFNOR (quelle que soit la source de ce soutien), si la France veut pouvoir continuer à maintenir son influence à l'échelle internationale.

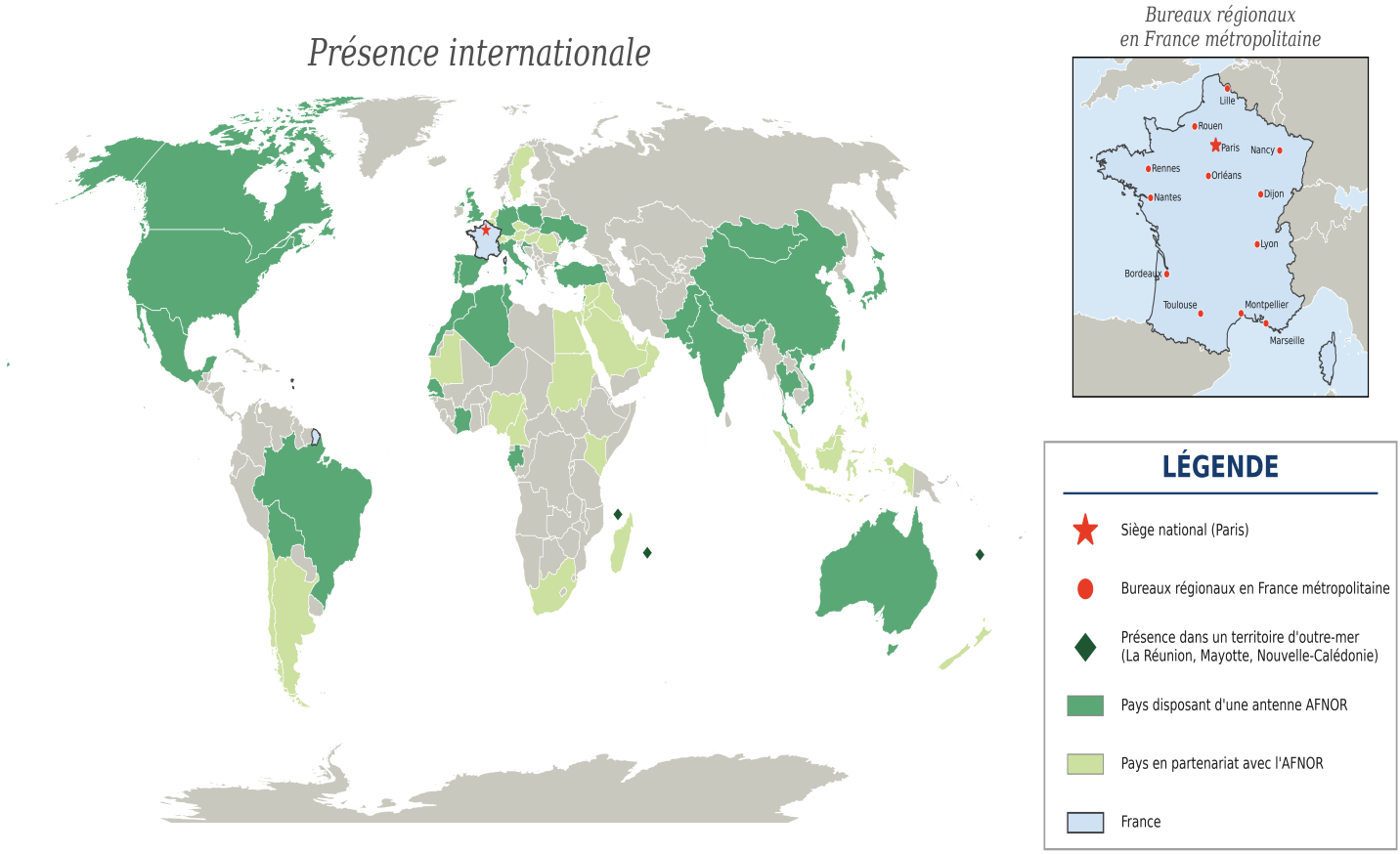
Le groupe AFNOR est représenté en régions par 14 bureaux répartis en 13 délégations en France[131], et à l'étranger dans 100 pays au travers de 32 antennes internationales[132] (cf. carte 1). À la fois outil de coordination de la normalisation à l'échelle nationale, l'AFNOR joue également un rôle dans la promotion de la place de la France sur l'échiquier international. Ainsi, les bureaux internationaux de l'AFNOR sont également le reflet des collaborations entre la France et ses proches partenaires économiques, sur tous les continents. L'étendue géographique de ces bureaux est également un indicateur de l'influence française en matière de normalisation. La présence de bureaux de l'AFNOR non seulement auprès de ses partenaires européens, mais également des principales puissances internationales dans le domaine de la normalisation (Allemagne, États-Unis, Royaume-Uni, Japon, Chine) souligne l'appartenance de la France au rang des grandes puissances normatives, tous domaines confondus. L'AFNOR est en charge de la gestion et de la promotion de la normalisation dans tous les domaines aux côtés des organismes agréés par le ministre chargé de l'industrie, comme les bureaux de normalisation sectoriels, afin de superviser ou de participer à l'élaboration de normes nationales, européennes ou internationales. À ce titre, l'AFNOR, en tant qu'entité exerçant une mission d'intérêt général, est investie de prérogatives relevant de l'autorité publique, notamment démontrée par l'autorité accordée à son directeur général pour homologuer les normes, leur permettant ainsi d'être incluses dans le répertoire officiel des normes françaises. Les normes nationales sont conçues en collaboration avec des commissions de normalisation (CN), qui rassemblent l'ensemble des parties impliquées souhaitant contribuer à ce processus. Pour cette raison, l'AFNOR s'engage à favoriser l'inclusion de tous les acteurs dans le système de normalisation français, qui ne se limitent pas exclusivement aux entreprises. Dans cette optique, l'AFNOR a établi des comités internes spécifiques pour mieux prendre en compte les perspectives des acteurs qui ne proviennent pas du secteur des entreprises, en particulier ceux qui ne sont pas liés à l'industrie, qui a historiquement été la principale

[131] Les bureaux régionaux de l'AFNOR sont présents dans les villes suivantes : Bordeaux, Dijon ; Lille ; Lyon ; Marseille ; Montpellier ; Nancy ; Nantes ; Orléans ; Paris, Rennes ; Rouen, Toulouse et Le Port (la Réunion)

[132] Les antennes internationales de l'AFNOR sont présentes dans les pays suivants : Algérie, Allemagne, Australie, Bolivie, Brésil, Canada, Chine, Corée du Sud, Côte d'Ivoire, Croatie, Espagne, États-Unis, France, Gabon, Inde, Italie, Japon, Liban, Maroc, Mexique, Mongolie, Pakistan, Pologne, Portugal, Royaume-Uni, Sénégal, Taïwan, Thaïlande, Tunisie, Turquie, Ukraine, Vietnam.

partie prenante de l'activité de normalisation. Dans les domaines partagés par de multiples secteurs, et dans les secteurs dépourvus d'organisme de normalisation sectorielle accrédité, l'AFNOR prend en charge la conception des projets de normes. Ainsi, l'AFNOR occupe une position centrale dans le système de normalisation français, ce qui lui confère un avantage pour promouvoir des positions influentes au sein des organes européens et internationaux. Cependant, cette position privilégiée ne doit en aucun cas entraver l'écoute ouverte des diverses perspectives exprimées, car cela constitue une condition essentielle pour le fonctionnement efficace de l'ensemble du système de normalisation français.

Carte 1 : Implantation mondiale du groupe AFNOR (2024)



Source : AFNOR (2024)

1.3.1 Le Comité de coordination et de pilotage de la normalisation (CCPN) et les comités stratégiques (co)

L'AFNOR n'est cependant pas le seul acteur du système français de normalisation. Parmi les autres organisés en charge du pilotage de la normalisation française internationale, on trouve tout d'abord le Comité de pilotage de la normalisation (CCPN). Le CCPN a pour mission de concevoir la stratégie de normalisation française, de définir les objectifs et les priorités globales des programmes de normalisation, ainsi que de veiller à leur alignement avec les politiques nationales, européennes et internationales, comme souligné par Elisabeth Lamure dans son rapport[133]. Pour ce faire, le CCPN rassemble l'ensemble des parties prenantes intéressées, afin de garantir une *« représentation équilibré »* »[134] de ces dernières. 50 % des membres sont composés de représentants d'entreprise et des bureaux de normalisation. Les membres restants sont composés à la fois des présidents de comités stratégiques et des représentants des autres parties prenantes de la société civile (syndicats, collectivités locales, administrations, associations de consommateurs et ONG). Le CCPN travaille en étroite collaboration avec l'ensemble des comités stratégiques (CO). Ces derniers, au nombre de 15, ont été créés afin d'assurer une représentation équilibrée des acteurs intervenant dans différents secteurs clés de l'économie. Chacun des cos doit définir une stratégie annuelle dans leur filière, coordonner les acteurs de leur filière et contribuer à préparer la position française concernant les sujets stratégiques présentés au CEN et au CENELEC, ainsi qu'à l'ISO et à l'IEC. Ce sont également les co qui mettent en place dans leurs domaines les « commissions miroirs » qui sont calquées sur les comités techniques du CEN ou de l'ISO afin de suivre des projets européens ou internationaux, comme la CN Infogéo pour les informations géographiques.

1.3.2 Les commissions de normalisation

Les commissions de normalisation sont créées afin de suivre et de participer aux débats internationaux en matière de normalisation dans des domaines spécifiques. Ils contribuent à la rédaction des projets de normes et sont en charge de porter les intérêts français sur la scène internationale dans leur domaine d'activité. La France en compte environ 1 200 dans tous les domaines techniques, qui rassemblent

[133] Elisabeth Lamure, « Où va la normalisation ? - En quête d'une stratégie de compétitivité respectueuse de l'intérêt général », Rapport d'information fait au nom de la commission des affaires économiques sur l'impact de la normalisation, Sénat (n° 627), 12 juillet 2017.

[134] Statuts du groupe AFNOR, Article 9, 10 décembre 2009.

environ 19 000 personnes. Ces commissions travaillent sur un mode ouvert, puisque n'importe qui, individu ou organisation, peut théoriquement les rejoindre. Cependant, il faut garder à l'esprit que participer a des travaux de normalisation à un coût qui varie de 1 730 euros à 6 200 euros par an. Le montant à régler varie en fonction de la nature et de la taille de l'organisme qui cherche à participer. Il existe cependant des exceptions inscrites dans le décret n °2021-1473 du 10 novembre 2021, permettant d'obtenir une exonération totale de droit. Cette exonération s'applique *« aux associations de consommateurs ou de protection de l'environnement agréées, aux PME de moins de 250 salariés ne dépendant pas à plus de 25 % d'un groupe de plus de 250 salariés, aux établissements publics d'enseignement et aux établissements publics à caractère scientifique et technologique »*[135]. Il faut également rajouter à cela l'ensemble des frais liés aux déplacements qu'occasionne la participation aux travaux de normalisation, notamment lors des réunions plénières des comités techniques. De ce fait, le poids financier associé à l'investissement au sein d'un comité de normalisation reste un des principaux freins à la participation des acteurs de la société civile à la normalisation.

1.3.3 Les bureaux de normalisation sectoriels (BN)

Les bureaux de normalisation sectoriels ont pour mission de coordonner et de participer à la création des normes françaises, européennes et internationales. Ils sont agréés par le ministère de l'Industrie. Les bureaux de normalisation sectoriels prennent en charge un certain nombre de commissions de normalisation, pouvant aller jusqu'à plusieurs dizaines, constituées d'experts désignés par les différentes parties prenantes impliquées dans les travaux de normalisation. Ces commissions sont chargées de rédiger ou de contribuer à la rédaction des documents de normes. Actuellement, il y a 22 bureaux de normalisation sectoriels agréés[136]. La taille et l'envergure des divers bureaux de normalisation sectoriels varient considérablement. Cependant, en réalité, seuls trois de ces bureaux sont responsables de 80 % de l'ensemble de l'activité de normalisation (il s'agit du département en charge de l'élaboration de normes de l'AFNOR en charge des comités techniques hors catégories, du bureau de normalisation de l'aéronautique et de l'espace [BNAE] et de l'Union de normalisation de la mécanique [UNM])[137]. De fait, certains bureaux de normalisation sont de très petite taille comparés à

---

[135] Élisabeth Lamure, « Où va la normalisation ? - En quête d'une stratégie de compétitivité respectueuse de l'intérêt général », Rapport d'information fait au nom de la commission des affaires économiques sur l'impact de la normalisation, Sénat (n° 627), 12 juillet 2017.

[136] Site officiel France Normalisation : https://www.francenormalisation.fr/les-acteurs-de-la-normalisation/les-bureaux-de-normalisation-sectoriels/

[137] Élisabeth Lamure, « Où va la normalisation ? - En quête d'une stratégie de compétitivité respectueuse de l'intérêt général », Rapport d'information fait au nom de la commission des affaires économiques sur l'impact de la normalisation, Sénat (n° 627), 12 juillet 2017.

d'autres, ce qui pourrait potentiellement limiter leur capacité à promouvoir efficacement leurs positions à l'échelle internationale[138]. Toutefois, il est important de noter que les bureaux de normalisation jouent un rôle essentiel en réunissant des experts et en assurant une écoute des besoins des acteurs économiques. La rédaction de normes exige des compétences solides et une bonne compréhension des parties prenantes concernées. Par conséquent, aussi petits soient-ils, les bureaux de normalisation sont primordiaux pour le maintien de l'influence française, en permettant de maintenir ce principe d'implication active des experts, tout en renforçant la représentativité des bureaux au sein des instances internationales. Aujourd'hui, le Comité national Information géographique et systèmes géodésiques, comité miroir français du TC/211 de l'ISO n'est pas rattaché à un BN spécifique et se retrouve par conséquent sous la tutelle du département d'élaboration des normes de l'AFNOR qui s'occupent des comités techniques hors catégories.

1.3.4 Le comité d'audit et d'évaluation

Le groupe d'évaluation et de vérification a la responsabilité de coordonner et d'évaluer les activités des organismes de normalisation, tout en supervisant les opérations du groupe AFNOR. Le comité d'audit et d'évaluation doit en priorité veiller au maintien de l'équilibre entre les différentes parties prenantes dans les activités de normalisation. Un point intéressant concernant le comité d'audit de l'AFNOR tient au fait que l'ensemble de ses membres sont eux-mêmes nommés par le conseil d'administration de l'AFNOR. Comme le révèle le rapport d'Élisabeth Lamure[139], certains observateurs ont souligné que la collusion entre les membres de l'AFNOR et ceux de ce groupe d'évaluation et de vérification soulève des préoccupations quant à son impartialité lorsqu'il s'agit d'auditer cette même entité. De plus, sa mission semble mal définie, car les statuts d'AFNOR étendent considérablement le rôle qui lui est attribué par le décret du 10 novembre 2021. En effet, les statuts d'AFNOR élargissent les fonctions à l'audit et à l'évaluation de l'ensemble *« des entités composant le système français de normalisation »*[140], dépassant ainsi le cadre des organismes de normalisation. Cela inclut notamment les comités stratégiques, le comité de coordination et de pilotage de la normalisation (CCPN), ou encore les autorités publiques. Au vu du poids déjà très important du groupe AFNOR au sein du système français de normalisation, on peut légitimement se demander s'il est vraiment judicieux qu'un comité

[138] Lydie Evrard, « Politique nationale de normalisation et stratégie pour la compétitivité de notre économie », Rapport remis au ministre de l'Économie, de l'Industrie et du numérique, décembre 2014.

[139] Elisabeth Lamure, « Où va la normalisation ? - En quête d'une stratégie de compétitivité respectueuse de l'intérêt général », Rapport d'information fait au nom de la commission des affaires économiques sur l'impact de la normalisation, Sénat (n° 627), 12 juillet 2017.

[140] Statuts du groupe AFNOR, Article 10, 10 décembre 2009.

d'audit et d'évaluation dont les membres sont directement nommés par le conseil d'administration de l'AFNOR se retrouve ainsi doté d'un droit de regard aussi large sur l'organisation de ce même système. Il apparaît évident que le maintien de l'impartialité de l'AFNOR est un enjeu important de la préservation de la compétitivité des propositions de normes françaises à l'international. Pour ce faire, conserver un comité d'audit impartial doit être une priorité. Ainsi, à l'avenir, une modification des statuts AFNOR ou une délégation d'une partie des prérogatives du comité d'audit et d'évaluation à un organisme public indépendant pourrait être nécessaire afin d'éviter tout problème de partialité dans les évaluations du fonctionnement de l'AFNOR.

1.3.5 Le délégué interministériel aux normes (DIN)

Comme le rappel Elisabeth Lamure, la fonction de délégué interministériel aux normes (DIN) est une spécificité française, qu'on ne retrouve dans aucun autre système de normalisation national[141]. Le rôle du délégué interministériel aux normes est de définir et *« mettre en œuvre la politique française des normes »*[142]. Il a autorité pour signer au nom du ministre les actes relatifs à la politique française de normalisation, à l'exception des décrets. Il est à la tête du groupe interministériel des normes. Cependant, le DIN n'est pas compétent concernant le contenu des normes votées dans les différents comités techniques, qui relève des experts. Le DIN a un rôle de commissaire du gouvernement défini par l'article 10 du décret du 10 novembre 2021, qui lui permet d'intervenir auprès de l'AFNOR en cas de dysfonctionnement majeur, cependant, il ne constitue pas une autorité de tutelle au sens strict puisque l'AFNOR n'est pas un établissement public. Il a également un rôle stratégique dans un domaine souvent sous-estimé, qui est de promouvoir l'emploi de la langue française et la traduction des documents normatifs avant leur validation. Le DIN peut aller jusqu'à s'opposer à l'homologation d'une norme non disponible en langue française. L'emploi de la langue française au sein des organes de normalisation est une composante importante du travail de normalisation, car seules les normes correctement traduites peuvent espérer être largement diffusées et appliquées une fois adoptées. Le délégué interministériel aux normes préside également le groupe interministériel aux normes (GIN). Ce dernier a pour mission de proposer au ministre des orientations pour la politique française des normes,

[141] Elisabeth Lamure, « Où va la normalisation ? - En quête d'une stratégie de compétitivité respectueuse de l'intérêt général », Rapport d'information fait au nom de la commission des affaires économiques sur l'impact de la normalisation, Sénat (n° 627), 12 juillet 2017.

[142] Décret n° 2021-1473 du 10 novembre 2021, portant modification du décret n° 2009-697 du 16 juin 2009 relatif à la normalisation, article 3.

cependant, il n'a pas autorité pour proposer formellement au ministre une stratégie pour la politique de normalisation.

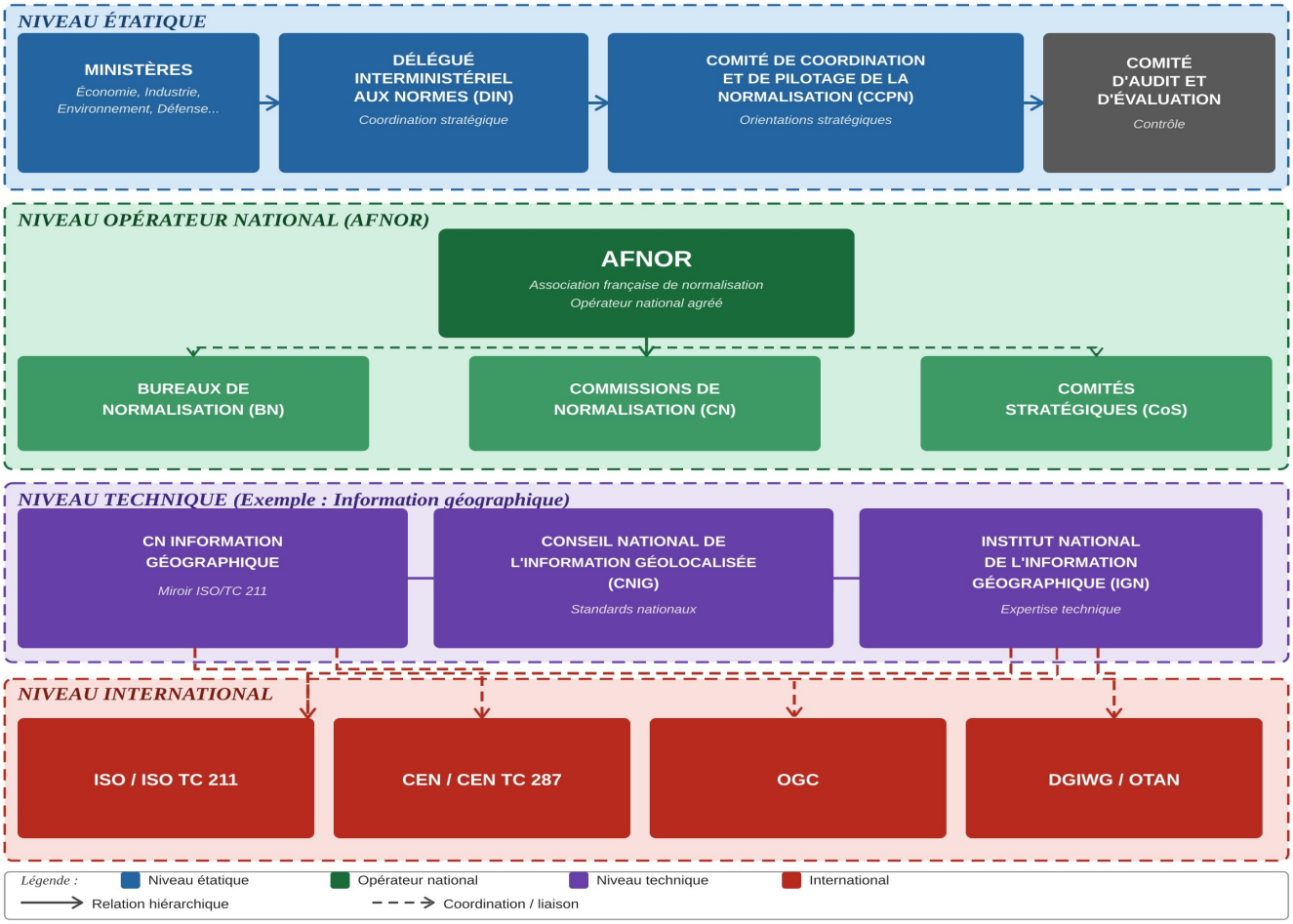
Comme il a été vu précédemment, le système français de normalisation s'articule autour d'un grand nombre d'acteurs institutionnels en charge de mettre en application la stratégie française de normalisation. Le système français de normalisation, hérité d'une implication de longue date de la France dans la normalisation internationale, fait l'objet d'une attention toute particulière de l'État dans le but de renforcer la compétitivité de la France sur la scène internationale. Le rôle central de l'AFNOR le consacre comme l'acteur majeur de la normalisation française, et ce, à toutes les échelles. Loin d'être un simple ambassadeur de l'État, le groupe AFNOR a ses propres intérêts à faire passer lorsqu'il s'agit de coordonner la normalisation française. Le rôle ambigu de l'AFNOR, notamment en ce qui concerne la mise à disposition des normes internationales, semble pouvoir être un frein à la diffusion de la normalisation au sein des entreprises françaises, ainsi que des acteurs de la société civile qui font face à une monétisation quasi systématique des normes. Il apparaît donc qu'il y a aujourd'hui un conflit d'intérêt certain du point de vue de l'AFNOR qui est à la fois en charge de la diffusion de la normalisation au sein des sociétés françaises, et qui dépend également de la vente des normes à ces mêmes sociétés pour vivre. Avec la diminution quasi constante des contributions de l'État au fonctionnement du groupe AFNOR, on est en droit de penser que la gratuité des normes n'est pas pour demain. Il convient donc de garder un œil sur le fonctionnement de l'AFNOR afin que le développement de normes ne devienne pas une fin en soi, dans le but de fournir des revenus à l'AFNOR par le biais de ces offres en certification notamment. Le cas de la normalisation des données géographiques est très éclairant sur l'effet pervers que peut engendrer le monopole de l'AFNOR sur la publication de normes.

En effet, la plupart des acteurs français de la normalisation des données géographiques sont des employés de l'Institut national de l'information géographique et forestière (IGN). C'est donc l'IGN qui fournit les fonds à ses experts lors des déplacements qu'engendre la participation à la normalisation internationale. Cependant, lorsque le travail normatif est terminé, et que les normes sont publiées, sous l'égide de l'ISO notamment, l'IGN ne touche pas un centime sur la vente de ces normes. De plus, lorsqu'une société appliquant lesdites normes cherche à obtenir une certification, c'est vers l'AFNOR et non l'IGN qu'elle se tourne, certification qui lui sera également facturée par l'AFNOR. Plusieurs solutions ont déjà été avancées pour tenter de contrebalancer le poids disproportionné de l'AFNOR dans le système français de normalisation. La nationalisation semble être une solution radicale qui permettrait un meilleur contrôle sur l'orientation stratégique de la normalisation française. Cependant, une telle solution entraînerait un coût très important pour l'État, en plus de risquer d'effrayer nombre de sociétés privées hostiles à une participation trop forte de l'État dans le processus normatif. Sociétés

qui seraient alors tentées de se tourner exclusivement vers des consortiums privés pour participer à ces processus, réduisant d'autant plus le nombre de sociétés pouvant se permettre d'y participer. Le coût de participation au sein des consortiums privés étant souvent prohibitif.

L'ouverture du rôle de l'AFNOR à la concurrence pourrait sembler également une solution, mais l'obligation de n'avoir qu'un seul organisme représentant au sein des organisations internationales de normalisation, telles que l'ISO, obligerait à déléguer à l'un de ces organismes ou à un ministère un droit de décision sur les projets de normes soutenus à l'internationale, créant un grand risque de conflit d'intérêts, de lobbying ou même de corruption de la part de certaines sociétés désireuses de pousser leur solution privilégiée à l'ISO. Si le système français de normalisation n'est donc pas parfait, l'AFNOR remplit tout de même son rôle avec diligence depuis près de 40 ans, et un renforcement du soutien de l'État aux acteurs de la normalisation, AFNOR comprises, reste probablement la meilleure solution pour cimenter l'influence française sur la scène internationale. En tant que représentant attitré de l'État français au niveau des instances internationales de normalisation, l'AFNOR est également présente au sein des organes de normalisation de l'Union européenne, à savoir le CEN, le CENELEC et l'ETSI. L'espace européen reste une échelle cruciale dans le développement des normes en France et sur le reste du continent. Les acteurs européens de la normalisation, non contents de faire partie des pays les plus anciens impliqués dans la normalisation internationale, ont également créé avec l'Union européenne un écosystème normatif sans équivalent dans le monde, en offrant aux sociétés européennes un espace de négociations régional bénéficiant à tous et permettant de préserver la souveraineté industrielle des États européens en soutenant des positions communes à l'échelle internationale.

Figure 3 : Architecture du système français de normalisation



Source : *Décret n° 2009-697 du 16 juin 2009 relatif à la normalisation*

1.4 L'Europe, acteur historique de la normalisation internationale

Seuls 10 % des normes publiées par l'AFNOR chaque année sont uniquement d'application nationale[143]. Ainsi, l'échelle internationale reste de loin l'échelon le plus important de l'étude des rivalités de pouvoir en matière de normalisation. Le monde ne montre aucun signe de développement d'une approche unique de la normalisation, il est donc utile de distinguer les différentes tendances de manière plus explicite. C'est justement ce qu'a fait le politiste Jay Tate, en proposant une lecture comparative de ces différences, en appliquant à la normalisation la grille des *« variété du capitalisme »* élaborée par Peter A. Hall et David Soskice. Il distingue des approches libérales, coordonnées et fondées sur la médiation de l'État, qu'il illustre par les cas britanniques, allemands, français, japonais et américain[144].En Europe, le contraste principal se situe entre le libéralisme des entreprises britanniques, la coordination des entreprises allemandes et le poids de l'État et de la médiation professionnelle des entreprises françaises. Les entreprises britanniques, qui favorisent la concurrence par les prix et l'ouverture des marchés, soutiennent l'utilisation de normes de gestion générales en lieu et place de normes précises relatives aux produits et aux processus de fabrication. L'unification européenne a aidé les entreprises britanniques à « exporter » leurs normes de gestion généralistes vers le continent tout en restant libres d'ignorer les normes continentales plus spécialisées et plus détaillées, que ce soit parce que les normes importées sont volontaires, qu'elles sont neutralisées par des accords de reconnaissance mutuelle ou qu'elles concernent des secteurs où le Royaume-Uni n'a pas d'entreprises nationales. À la suite de la sortie du Royaume-Uni de l'Union européenne, les instances normatives britanniques sont aujourd'hui entièrement décorrélées des obligations européennes en la matière. Cependant, le Royaume-Uni n'a pas déserté les instances européennes de normalisation pour autant et garde un statut d'associé au sein des instances de normalisation européennes. À l'inverse, les entreprises allemandes, tout en assimilant les normes de gestion britanniques, ont régulièrement transposé aux niveaux européen et international une grande partie de leur approche, notamment en matière de coordination de l'ensemble des normes détaillées relatives aux produits et aux processus de fabrication. Les entreprises allemandes hébergent plus de comités techniques, tant au sein du CEN/CENELEC que de l'ISO/CEI[145],

---

143 Pernollet Jacques, « Le processus d'élaboration des normes techniques aux plans national, communautaire et international », *Les Petites Affiches*, n° 18, 11 février 1998, pp. 12-14.

144 Tate Jay, « National Varieties of Standardization », in Hall Peter A. et Soskice David (dir)., Varities of Capitalism : The Institunal Foundations of Comparative Advantage, Oxford, Oxford University Press, 2011, pp. 442 – 473.

145 Dong Geunh Choi et Puskar Erik, « A Review of U.S.A. Participation in ISO and IEC, Standards Coordination Office Laboratory Programs », National Institute of Standards and Technology (NIST), U.S. Department of Commerce

que les entreprises de n'importe quel autre pays. Les entreprises françaises, qui cherchent à étendre leurs réseaux interentreprises au niveau européen, soutiennent les directives et les mandats de l'UE ainsi que d'autres formes de médiation de la normalisation similaire à celles qui existent en France. Selon Tate, la normalisation européenne représente « un amalgame d'approches nationales disparates »[146], dont le principal résultat a été de combiner ces alternatives plutôt que de les abolir.

Dans le reste du monde, l'approche coordonnée de l'Union européenne en matière de normalisation fait face à un ensemble d'économies de marché dirigistes en Asie de l'Est, sur le modèle du Japon et de la Chine, ainsi qu'à une approche hyperlibérale de la normalisation ancrée aux États-Unis[147]. Ces variétés convergent-elles simplement parce que les entreprises de tous ces pays participent à un trio d'organisations internationales basées à Genève, l'Organisation internationale de normalisation (ISO), le Comité électrotechnique international (CEI) et l'Union internationale des télécommunications (UIT-T) ? Pas vraiment, puisque l'adhésion à ces organisations est réservée aux pays (et non aux entreprises ou aux individus), ce qui limite l'influence des entreprises et conglomérats de grands pays, tels que le Japon et les États-Unis. Comme l'a déclaré Raymond Kammer, directeur du NIST (National Institute of Standards and Technology), en 1998 : *« Les normes ISO et CEI ont tendance à répondre aux besoins européens et seulement de temps en temps aux besoins de l'industrie américains »*[148]. On pourrait en dire autant des besoins japonais, alors même que les entreprises japonaises ont été des participantes avides, envoyant souvent des délégations bien plus importantes, et bien plus coûteuses, que n'importe quel autre pays. Ainsi, depuis 1991, l'écosystème international de normalisation est devenu de plus en plus un avant-poste du système européen de normalisation. Après deux années de collaboration informelle, « l'accord de Vienne » entre le CEN et l'ISO et « l'accord de Lugano » entre le CENELEC et la CEI ont été signés, ce dernier a été révisé par un « accord de Dresde » en 1996. Les normes nationales (BSI, DIN, AFNOR, etc.), régionales (CEN, CENELEC) et internationales (ISO, CEI) européennes sont aujourd'hui étroitement coordonnées les unes avec les autres, à un degré sans commune mesure avec d'autres régions du monde. Ainsi, non contents de profiter d'un avantage historique dans le domaine de la normalisation lié à leur implémentation précoce dans les mécaniques de normalisation industrielles et leur institutionnalisation internationale à partir de 1946, les acteurs européens profitent aujourd'hui de l'Union européenne pour coordonner à l'échelle du continent leurs travaux de normalisation. Cela permet une interopérabilité extrêmement poussée au sein

(NISTIR 8007), juin 2014.

146 Tate Jay, « National Varieties of Standardization », in Hall Peter A. et Soskice David (dir)., Varities of Capitalism : The Institunal Foundations of Comparative Advantage, Oxford, Oxford University Press, 2011, p. 469.

147 American National Standards Institute (ANSI), « Understanding the U.S. Voluntary Consensus Standardization and Conformity Assessment Infrastructure », 2020. https://www.standardsportal.org/usa_en/standards_system.aspx

148 ASTM (American Society for Testing and Materials). *Standardization News*, n° 26, juin 1998.

des industries européennes, tout en assurant le respect des exigences mutuelles et le règlement des éventuels conflits par des négociations intraeuropéennes.

Cependant, bien que les entreprises européennes aient fait des efforts très importants pour harmoniser les normes nationales officielles au cours des années 1990. Les normes restent différentes dans les plus grands pays. Le Japon (qui a pourtant déployé des efforts considérables pour harmoniser le JIS [Japanese Industrial Standards] avec les normes internationales au cours des années 1990)[149] et les États-Unis (qui ont fait relativement peu d'efforts pour modifier les normes nationales) sont encore moins tributaires des normes internationales. En outre, la Chine et d'autres pays asiatiques qui se développent rapidement ont cherché, dans les limites fixées par l'OMC, le FMI et d'autres organisations internationales, à imiter l'utilisation agressive des normes nationales par le Japon[150]. Avec le développement des Nouvelles Routes de la Soie (NRS), la Chine, en particulier, a accru de façon spectaculaire son intégration au sein des divers organismes internationaux de normalisation ces dernières années.

Ainsi, les institutions nationales de normalisation continuent de différer, restant au moins aussi diverses que les gouvernements sous lesquels elles opèrent. Les institutions de normalisation peuvent être libérales, qu'il s'agisse d'organismes de commercialisation (BSI en Angleterre) ou d'organismes d'accréditation qui certifient des organismes de normalisation concurrents (American National Standards Institute), elles peuvent servir de point central de la coordination nationale, qu'il s'agisse d'un coordinateur autonome de groupements industriels (DIN en Allemagne) ou d'un groupe de réflexion gouvernemental (JIS au Japon), ou il peut s'agir d'associations de professionnels qui servent de médiateurs entre les entreprises (comme l'AFNOR en France). Les institutions de normalisation libérales s'appuient principalement sur des professionnels relativement autonomes, les institutions de normalisation coordonnées s'appuient principalement sur des représentants organisationnels d'associations industrielles et les institutions de normalisation par médiation s'appuient principalement sur des tierces neutres pour concilier les différences entre les entreprises. Même lorsque les entreprises de certains petits pays européens (notamment les Pays-Bas) ont décidé d'abandonner les travaux de normalisation nationaux au profit des travaux sur les normes européennes, elles n'ont pas fermé leur organisme national de normalisation ni abandonné leurs efforts pour imposer des préférences nationales.

---

149 Eto Manabu, « Historical Development of Industrial Standardization in Japan as the Background of the Current Standards and Conformity Assessment Policy » (工 業標 準化 政 策 の 変遷 と基準認 証 政 策), *The Journal of Science Policy and Research Management*, n°22, 2007.

150 Gibson Christopher S., « Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in International Standards », Boston, Massachusetts, Suffolk University Law School, *Legal Studies Research Paper Series* (Research Paper 07-39), 31 octobre 2007.

Plus important encore, les approches nationales quant à l'objectif des normes sont de plus en plus contradictoires. Ainsi, Tate résume cette opposition en deux formules : dans les économies de marché libérales, *« les stratégies d'entreprise considèrent les normes comme un bien ou un service exclusif à commercialiser comme n'importe quel autre »*, tandis que dans les économies de marché coordonnées, elles *« traitent au contraire les normes comme une infrastructure au service d'une coopération plus approfondie »*[151]. En Grande-Bretagne, les normes les plus importantes consistent en un service commercial permettant de réduire les coûts d'assurance et de garantie. Aux États-Unis, précisément en raison de leur approche très libérale, les normes sont devenues des éléments de propriété intellectuelle, tour à tour protégés et contestés. Les entreprises allemandes quant à elles, sont rapidement devenues les leaders mondiaux dans la création d'une infrastructure transnationale de normalisation, en transférant leur travail de normalisation national habituel aux niveaux européen et international qui, à leur tour, restent étroitement intégrés à leurs normes nationales plus spécialisées. Au Japon, où les entreprises recherchent une production de masse et souple, la coordination des normes se distingue par le degré d'intégration des normes nationales et des normes des groupements industriels avec des innovations progressives au niveau de chaque usine, de façon à faciliter la concurrence oligopolistique[152]. Enfin, la France, où domine la médiation de l'État, apparaît tantôt libérale, tantôt coordonnée, selon que cette médiation est ou non étatiste[153] (cf. carte 2).

Les normes sont des éléments de plus en plus cruciaux de la concurrence économique dans de nombreux secteurs. L'une des conséquences de cela est que les règles et les institutions nationales par lesquelles les normes sont créées deviennent elles-mêmes de plus en plus des objets d'activité stratégique. Dans une perspective plus large, les avancées coordonnées du marché, tel que l'harmonisation européenne, et les avancées du marché libéral fondées sur des normes propriétaires, peuvent être considérées comme les premières étapes d'une rivalité permanente qui semble loin d'être terminée. La normalisation des données géographiques à l'échelle mondiale s'inscrit dans cet écosystème d'approches concurrentes en matière de normalisation, tant au niveau de l'ISO que des consortiums privés, tels que L'Open Geospatial Consortium (OGC).

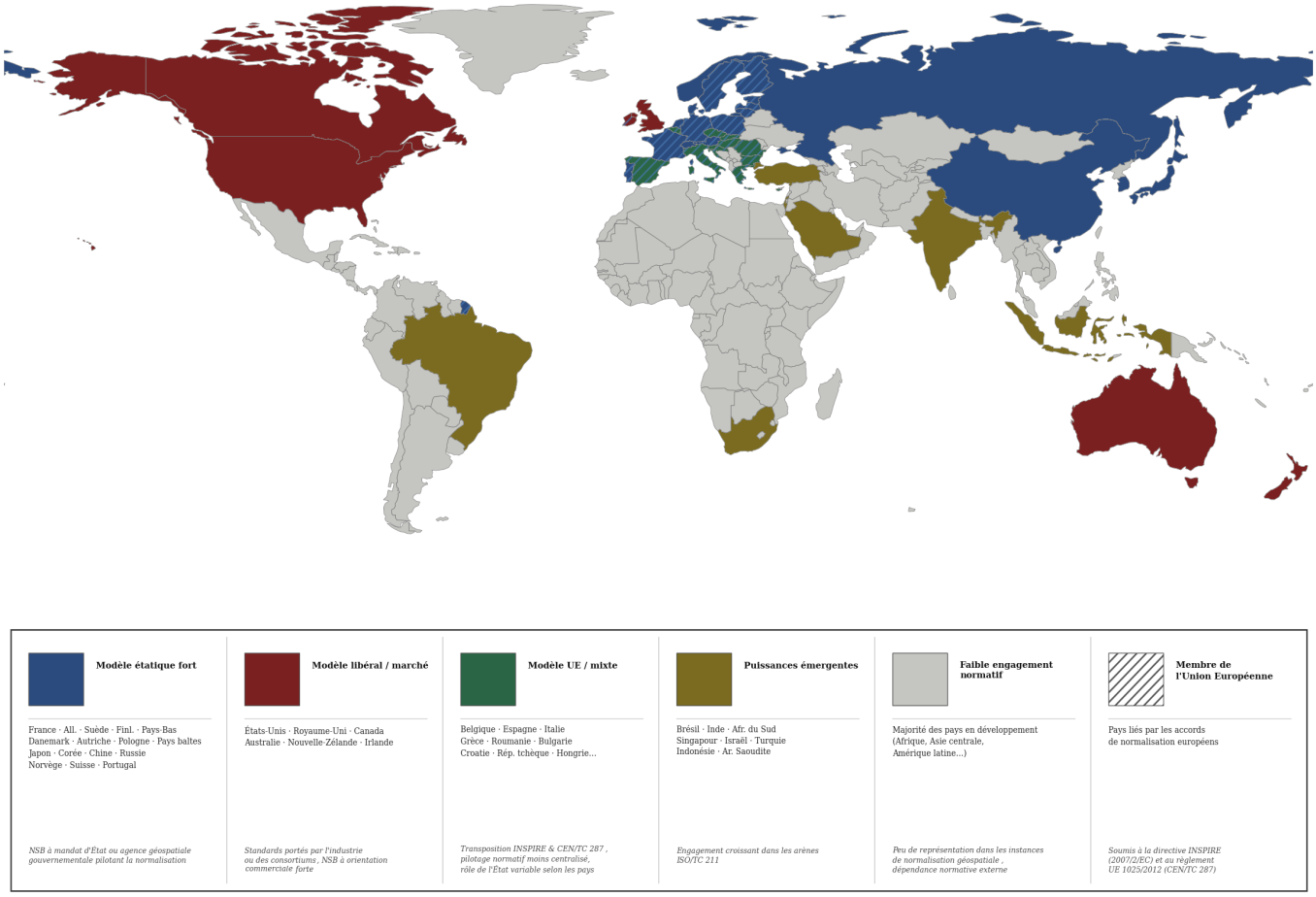
---

151 Tate Jay, « National Varieties of Standardization », op. Cit., p.472.

152 Nagano Juichi et Fukuda Yasukazu, « The Japanese Standardization Systems: History and Current Status », *IEEE Communications standards Magazine*, n° 2, septembre 2018.

153 Tate Jay, « National Varieties of Standardization », op. Cit., p.472

Carte 2 : Modèles nationaux d'organisation de la normalisation géospatiale (2023)



Source : ISO/TC 211, OGC, AFNOR, entretiens terrain 2022–2023. Classification de l'auteur

2. Les spécificités de l'information géographique en matière de cybersécurité et de normalisation

Les données géographiques représentent un domaine spécifique de la normalisation dotée d'acteurs propres et animé par une communauté diverse provenant du monde entier. À l'heure où la majorité des données géographiques sont produites et manipulées sur des supports numériques, la normalisation de ces données a suivi ces évolutions et s'occupe du développement de méthodes nécessaire à l'échange et au traitement de ces données. De même, à l'heure où les capteurs de toutes natures se multiplient pour capturer des données géographiques (optiques, radar, laser…), la normalisation de ces capteurs et de leurs données tient une place importante dans les projets de normes en développement au sein des instances internationales de normalisation. Le domaine des données géospatiales est également transverse au vu de la très large étendue des applications possibles de ces données. Le domaine des technologies spatiales en particulier, avec la multiplication des satellites et capteurs qui les accompagnent, développe de nombreuses normes en étroites collaborations avec les experts du domaine géographique. À l'heure de l'ubiquité informatique, les données géographiques sont entrées de plain-pied dans le domaine des technologies de l'information et de la communication et les normes de la communauté des informations géographiques et géodésiques avec elles. Cette situation a participé à profondément modeler l'environnement des normes géographiques ces vingt dernières années, et ces dernières, qui se développent désormais en étroite collaboration avec des domaines technologiques de pointe, comme l'intelligence artificielle ou les technologies quantiques.

2.1. La normalisation des données géographiques

Les données géographiques disposent de leur propre comité technique au sein de l'ISO, le Comité technique 211 (TC 211), intitulé « information géographique, géomatique ». La France dispose d'un comité miroir de l'ISO/TC 211 chargé de représenter les intérêts français en matière de normalisation des données géographiques sur la scène internationale, il s'agit de la commission de normalisation (CN) « Information géographique et systèmes géodésiques ».

Le champ d'application de l'ISO/TC 211 est très large et vise à remplir plusieurs objectifs clés : la modélisation et la documentation de l'information géographique, la facilitation de la recherche, de l'accès et de l'intégration de l'information géographique grâce aux services Web, l'intégration de l'information géographique à la vie quotidienne, et à accentuer la coordination dans certains domaines spécifiques où l'information géographique est une composante importante et où plusieurs disciplines sont impliquées. Ces travaux visent à établir un ensemble structuré de normes pour les *« informations*

concernant des objets ou des phénomènes qui sont directement ou indirectement associés à un emplacement par rapport à la Terre »[154]. Ces normes peuvent spécifier, pour l'information géographique, des méthodes, des outils et des services pour la gestion des données (y compris la définition et la description), l'acquisition, le traitement, l'analyse, l'accès, la présentation et le transfert de ces données sous forme numérique/électronique entre différents utilisateurs, systèmes et lieux. Les travaux du TC 211 sont liés, dans une large mesure, au développement de normes appliquées au domaine des technologies de l'information et des données, et visent à fournir un cadre pour le développement d'applications sectorielles utilisant des données géographiques.

Aujourd'hui, les informations géographiques sont disséminées sur toute la planète et employées par un large ensemble d'organisations publiques comme privées. Les exemples d'applications des données géographiques sont légion, on peut citer pêle-mêle : la lutte contre les catastrophes naturelles, l'organisation du territoire, la planification et la conduite d'opérations militaires, ou encore la gestion des flux de biens et de personnes. Les avantages que les différents acteurs tirent des données géographiques viennent non seulement de leurs mises à disposition, mais également, et souvent avant tout, de leur exploitation. Il ne suffit donc pas de savoir générer de la donnée, mais d'en maximiser l'exploitation et la diffusion. Le tout afin d'en tirer un savoir, qui doit être communiqué aux acteurs concernés. Cela est particulièrement vrai concernant les citoyens, qui ne sont pas nécessairement armés pour interpréter correctement les données géographiques brutes. Il convient donc de développer des outils de visualisation adéquats, capables de transmettre les données et d'offrir des outils permettant leur exploitation. La normalisation des données joue un rôle fondamental dans ce processus en permettant le déploiement d'un socle commun de référence, capable de servir de support à tous les éléments permettant la production, la dissémination et l'exploitation des données.

Le déploiement à travers le monde d'infrastructures de données géographiques (ou Spatial Data Infrastructure en anglais SDI) a contribué à accroître la disponibilité des informations géographiques dans le monde. Les Nations unies reconnaissent que cette approche contribue à la mise en œuvre des objectifs de développement durable (ODD). Le Comité d'experts des Nations unies sur la gestion mondiale de l'information géospatiale (UN's Committee of Experts on Global Geospatial Information Management : UN-GGIM) a élaboré le cadre intégré d'information géospatiale (Integrated Geospatial Information Framework : IGIF) qui reconnaît que les normes sont un élément clé d'un écosystème complexe couvrant différents domaines, tels que *« la gouvernance, la politique, l'économie, les données, l'innovation, les partenariats, l'éducation et l'engagement »*[155].

---

[154] Mats Ahlin, « ISO TC 211 Strategic Business Plan 2023 », 8 décembre 2022

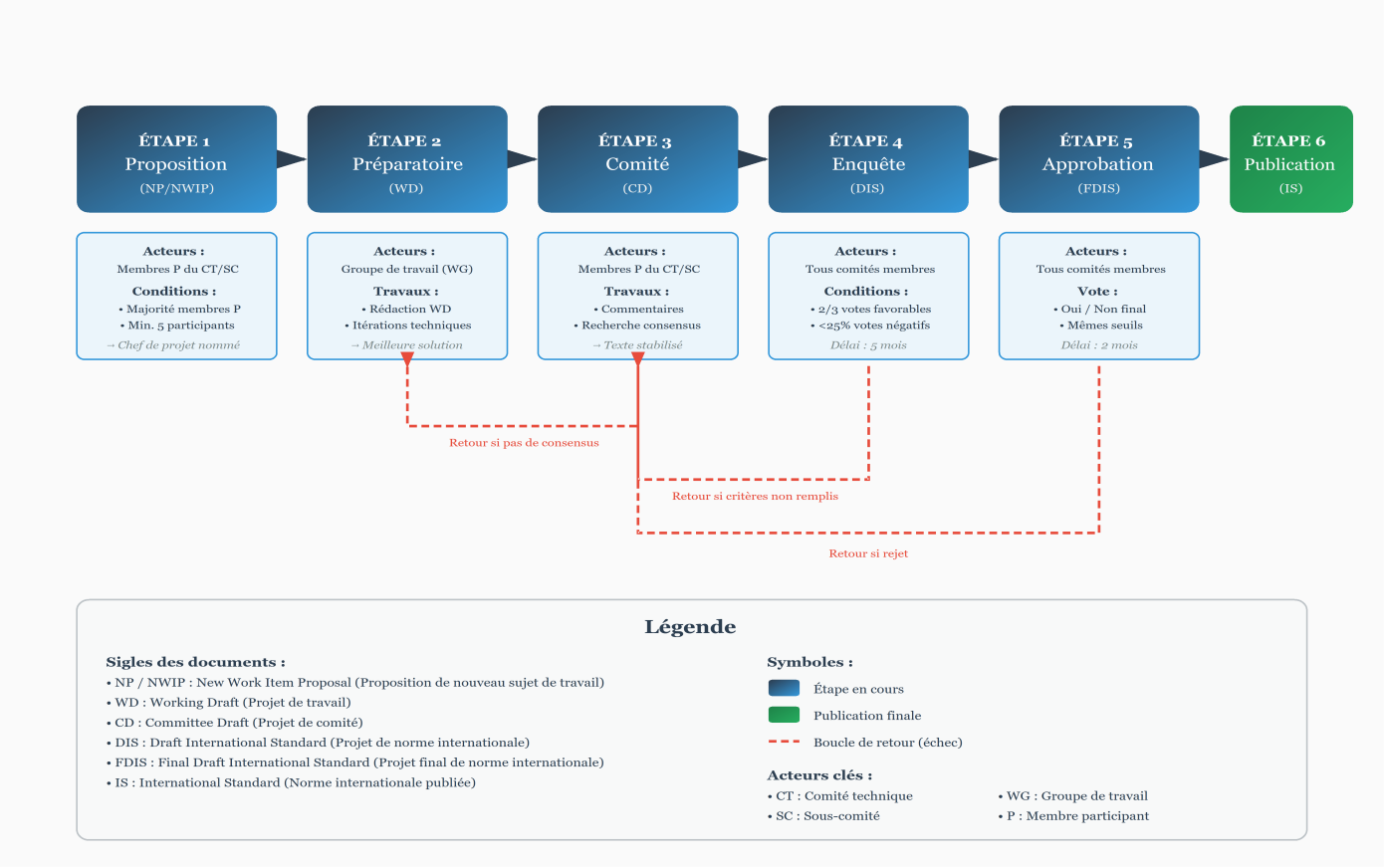
[155] OGC, ISO/TC 211 et L'IHO, « A Guide to the Role of Standards in Geospatial Information Management », New York, NY, août 2021.

Nous vivons dans un monde de plus en plus connecté, et cela vaut également pour les informations géographiques. L'interconnexion entre les capteurs et les citoyens a amené à la production continuelle d'un large volume de données géographiques accessibles sur le Web. Ces données sont de plus en plus détaillées, actualisées et souvent accessibles instantanément. Le traitement automatisé de ces données est rendu possible par leur normalisation, qui, par extension, nous donne accès au savoir qu'elles renferment. L'information géographique tend à être de plus en plus intégrée à d'autres domaines, tels que les transports intelligents, la construction, la gestion des villes et les instituts de statistiques nationaux. Récemment, plusieurs de ces domaines ont adopté le concept de « jumeau numérique » pour envisager des copies numériques à l'échelle de la ville des modèles d'infrastructure, de transport, de service urbain, enrichies de données provenant de capteurs en temps réel ou quasi réel et de la communauté des citoyens. L'utilisation de normes permet d'intégrer ces données.

Le fondement du fonctionnement de l'ISO/TC 211, comme de l'ensemble des comités techniques de l'ISO est la négociation. En effet, c'est la recherche consensus au sein des participants des sous-comités qui constitue la condition sine qua non de l'adoption d'une norme, et qui garantit également sa légitimité par la négociation des experts qui préside à sa création. Afin de s'assurer que le consensus au sein des experts réunis, mais également, au sein de la communauté des utilisateurs de données géographique, soit respecté, le développement de normes est divisé en plusieurs étapes qui doivent être scrupuleusement suivies (sauf en cas de processus accéléré, une situation exceptionnelle qui intervient généralement pour faire valider une norme de facto déjà largement adoptée par le marché), et dont le non-respect peut entraîner à tout moment l'annulation du projet de norme.

2.1.1 Les différentes étapes de l'adoption d'une norme internationale

Figure 4 : Processus d'adoption d'une norme internationale ISO



Source : *Directives ISO/IEC, Partie 1 – Procédures pour les travaux techniques (2021)*

1. Étape de proposition

La première étape de l'élaboration d'une norme internationale consiste à confirmer qu'une norme internationale est bien nécessaire. Une proposition de nouvel élément de travail (NP) est soumise au vote des membres du CT (Comité Technique) ou SC (Sous-Comité) concerné afin d'évaluer l'inclusion de l'élément de travail dans le programme de travail du Comité. La proposition est acceptée si une majorité des membres P (Participant) du CT/SC vote en sa faveur et si au moins cinq membres P déclarent leur engagement à participer activement au projet. À ce stade, un chef de projet responsable de l'élément de travail est normalement nommé.

2. Étape préparatoire

Habituellement, un groupe de travail d'experts, dont le président (organisateur) est le chef de projet, est mis en place par le CT/SC pour la préparation d'un projet de travail. Des projets de travail successifs peuvent être examinés jusqu'à ce que le groupe de travail soit convaincu d'avoir élaboré la meilleure solution technique au problème traité. À ce stade, le projet est alors transmis au comité de tutelle du groupe de travail afin qu'il trouve un consensus parmi les membres P.

3. Étape du comité

Dès qu'un premier projet de comité est disponible, il est enregistré par le Secrétariat central de l'ISO. Il est ensuite distribué pour commentaires et, si nécessaire, pour vote, par les membres P du CT/SC. Des projets de comité successifs peuvent être examinés jusqu'à ce qu'un consensus soit atteint sur l'aspect technique. Une fois le consensus atteint, le texte est arrêté pour être soumis en tant que projet de norme internationale (draft international standard : DIS).

4. Étape de l'enquête

Le DIS est diffusé à tous les comités membres de l'ISO par le Secrétariat central de l'ISO pour vote et commentaires dans un délai de cinq mois. Il est approuvé pour être soumis en tant que projet final de norme internationale (final draft international Standards FDIS) si une majorité des deux tiers des membres P du TC/SC est favorable et si moins du quart du nombre total de votes exprimés est négatif. Si les critères d'approbation ne sont pas remplis, le texte est renvoyé au comité d'origine.

5. Étape de validation

Le projet final de norme internationale (FDIS) est diffusé à tous les comités membres de l'ISO par le Secrétariat central de l'ISO pour un vote final Oui/Non dans un délai de deux mois. Si des commentaires techniques sont reçus pendant cette période, ils ne sont plus pris en compte à ce stade, mais enregistrés pour être examinés lors d'une future révision de la norme internationale. Le texte est approuvé en tant que norme internationale si une majorité des deux tiers des membres P du TC/SC est en faveur et si moins d'un quart du nombre total des votes exprimés est négatif. Si ces critères d'approbation ne sont pas remplis, la norme est renvoyée au CT/SC d'origine pour réexamen à la lumière des raisons évoquées à l'appui des votes négatifs reçus.

6. Étape de la publication

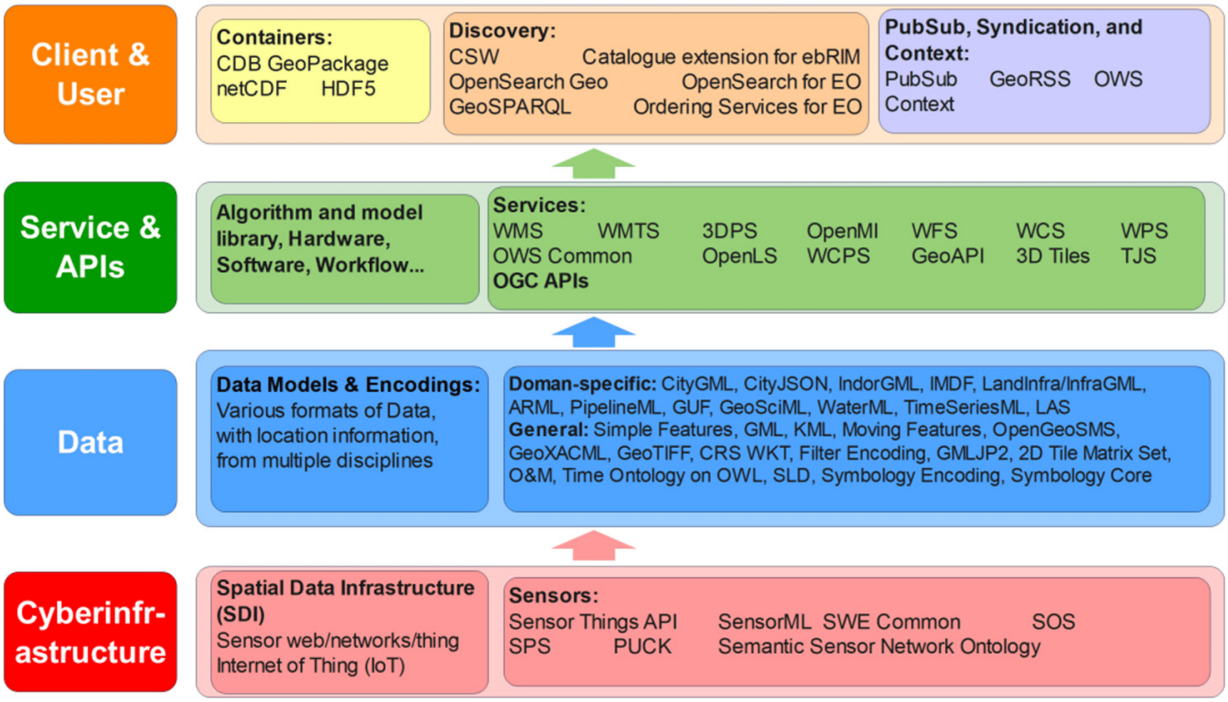
Une fois qu'un projet final de norme internationale a été approuvé, seules des modifications rédactionnelles mineures, si nécessaire, sont introduites dans le texte final. Ce dernier est alors envoyé au Secrétariat central de l'ISO, qui publie la norme internationale.

2.2 L'intérêt des normes en matière d'information géographique

Les normes d'information géographique constituent les fondations qui rendent possibles le partage des données et l'interopérabilité, et constituent une base pour d'autres domaines techniques qui ont besoin d'une représentation numérique du monde. Dans la mesure du possible, les normes en matière d'information géographique s'appuient sur les normes des technologies de l'information et de la communication, et d'autres domaines qui ne sont pas spécifiquement géographiques. Les normes spécifiques à un domaine s'appuient ensuite sur les normes géographiques et, ensemble, elles constituent les piliers de l'interopérabilité. Les normes permettent l'interopérabilité grâce à des définitions et à une structure cohérentes pour les différents éléments qui composent les données

géographiques numériques et leur diffusion. La classification des normes offertes par l'OGC donne un bon aperçu des différents types de normes en matière d'information géographique (cf. Figure 5)[156]. Ainsi, les normes permettent d'harmoniser les infrastructures numériques (les capteurs et leur interconnexion), les données et les métadonnées (aspect sémantique), l'encodage (la syntaxe) ainsi que l'accès et le traitement (les services Web et les API).

Figure 5 : Architecture des normes OGC



Source : *Open Geospatial Consortium (2021)*

Ensemble, les aspects différents organismes de normalisation rendent l'information géographique plus fine, plus accessible, plus interopérable et plus réutilisable. À titre d'exemple : l'Internet Engineering Task Force (IETF) normalise l'Internet et certains des transferts d'informations qu'il permet. Tandis que les normes du World Wide Web Consortium (W3C) couvrent la majeure partie de l'environnement Web, et L'ISO/TC 211 et l'OGC fournissent des normes spécifiques à l'information géographique, telle que la représentation de la localisation (schéma géospatial), la géodésie et les systèmes de référence des coordonnées, ainsi que des profils de normes informatiques génériques, l'Organisation météorologique mondiale (OMM), l'Organisation hydrographique internationale (OHI)

[156] Site officiel de l'OGC : https://www.ogc.org/standards/

et le Defence Geospatial Information Working Group (DGIWG) fournissent des normes pour leurs domaines en utilisant cette base commune de normes géographiques.

De nombreux bénéfices sont tirés de la normalisation des données géographiques, entre autres en améliorant l'accès aux services publics, facilitant l'intervention des services de secours en cas d'accident, et réduisant le coût environnemental des transports de biens et services en optimisant leur déplacement. Les bénéfices globaux s'appliquent à l'ensemble des domaines normalisés, en particulier concernant les systèmes d'information et les technologies qui leur sont rattachés. Par exemple L'IS 19135-1 spécifie les procédures à suivre pour établir, maintenir et publier des registres d'identifiants et de significations uniques, non ambigus et permanents qui sont attribués à des informations géographiques. Les normes permettent également d'améliorer la fiabilité des systèmes grâce à la réutilisation de composants éprouvés, mais également de réduire la dépendance à l'égard des fournisseurs propriétaires et de rendre possible l'interopérabilité entre les systèmes grâce à l'utilisation de schémas et d'interfaces communs. La normalisation des terminologies et des définitions de données permet une meilleure compréhension des données au sein de la communauté des utilisateurs et des producteurs de données géographiques à travers le monde. Enfin, la normalisation des métadonnées facilite le classement et la recherche des données. Certains avantages sont spécifiques au domaine de l'information géographique, comme par exemple, la capacité d'intégrer des données de localisation grâce à l'utilisation de systèmes de référencement géospatiaux normalisés.

Un des principaux buts recherchés par les participants aux différents groupes de travail sur les normes tient principalement aux gains financiers offerts par l'interopérabilité qu'offre leur adoption. Le bénéfice des normes n'est plus à démontrer et plusieurs études sont déjà parues sur les avantages liés à l'adoption de normes pour les utilisateurs comme pour les sociétés privées travaillant dans le domaine des technologies de l'information[157], comme dans celui de la production de données géographiques[158]. Un impératif qui motive l'exigence d'interopérabilité des systèmes est la nécessité d'économiser de l'argent et des ressources en réutilisant les données géospatiales. Cependant, les interfaces de données et de logiciels utilisées par les différents systèmes sont souvent dissemblables et incompatibles. De plus, les différents systèmes ont souvent des plateformes logicielles et matérielles uniques. Dans un tel environnement, les normes d'interopérabilité géospatiale et les spécifications des formats de données et des interfaces d'application sont présentées comme un moyen de surmonter les obstacles à l'interopérabilité des systèmes. Ces normes fournissent aux utilisateurs, aux gestionnaires et aux opérateurs des directives relatives au format des données et à l'interopérabilité des applications afin de

[157] Delphi Group, « The Value of Standards: A Delphi Study », Boston (Massachusetts), juin 2003.

[158] Boozz Allen Hamilton, « Geospatial Interoperability Return on Investment Study », National Aeronautics and Space Administration (NASA), Geospatial Interoperability Office, Avril 2005.

combler les différences sémantiques et syntaxiques posées par un environnement informatique hétérogène.

De nombreuses agences étatiques, ainsi que des entreprises privées et des organismes à but non lucratif, sont engagées dans la collecte et le maintien de données géospatiales précises. De plus, un nombre croissant de fournisseurs commerciaux vendent une variété de plus en plus riche de données spatiales pour répondre à divers besoins. Des fournisseurs qui développent les bases de données des tracés des rues utilisées dans les GPS et dans les globes virtuels sur Internet, tels que Google Earth ou les systèmes de navigation en ligne, comme Google Maps ou Waze. Ces données sont transmises à un nombre croissant d'appareils, dont les ordinateurs portables et les téléphones. Pour que ces services soient disponibles sur un large éventail de dispositifs et de systèmes d'exploitation, il est nécessaire qu'ils communiquent tous entre eux, ou interopèrent. En créant des applications avec des spécifications ouvertes et en normalisant les données pour qu'elles soient conformes à un certain contenu et à une certaine structure définie au préalable, la communauté des utilisateurs et des producteurs de données peut profiter d'une plus grande interopérabilité. La capacité des différents systèmes à interagir signifie que les personnes et les agences nationales ou privées peuvent recombiner des informations disparates (comme l'imagerie de la couverture terrestre de la NASA) et les appliquer de manière nouvelle et imprévue à un grand nombre de problèmes. Une fois appliquée à des problématiques de santé publique ou de sécurité nationale, l'interopérabilité offerte par la normalisation des données géographiques peut sauver des vies. Elle peut également entraîner une meilleure gestion des biens et ressources publics, entraînant d'importantes économies pour les contribuables.

Par conséquent, l'impact de l'interopérabilité des données géographiques sur le gouvernement et la société est considérable. L'impact sur l'industrie est tout aussi important. Les organisations ont de plus en plus tendance à intégrer l'information géospatiale dans leurs activités courantes, car elles reconnaissent que l'information géographique est un élément clé de l'intelligence économique et de l'infrastructure d'information. Au fur et à mesure que les fournisseurs de technologies géospatiales pénètrent de nouveaux marchés à l'étranger, ils se voient obligés de prendre en charge les normes locales et internationales, ce qui entraîne un soutien accru de ces normes dans leurs produits.

Cependant, l'adoption de normes nouvelles peut prendre du temps, et les différents acteurs publics comme privés sont parfois réticents à adopter de nouvelles normes. En effet, choisir d'adopter unilatéralement une norme technique n'est pas sans risques. L'immaturité de certaines normes, lorsque ces dernières n'ont pas encore atteint un stade de développement suffisamment avancé, est un des facteurs qui entre en ligne de compte dans la non-adoption de certaines normes. Certains des risques peuvent également être attribués à une méconnaissance du processus de normalisation et de sa pratique, qui comporte des protocoles très spécifiques peu connus en dehors de la communauté de normalisation.

Enfin, alors que l'Internet est aujourd'hui omniprésent et modifie le prix de l'information, ces risques montrent qu'il existe une tension entre les notions traditionnelles de propriété intellectuelle et l'incertitude entourant la future économie de l'information. La non-adoption d'une norme ou le refus de participer à des travaux de normalisation, notamment du point de vue des industriels, est souvent justifié par un certain nombre de risques qui peuvent naître de l'adoption précoce de normes dans certains domaines.

Tout d'abord, le manque de soutien de l'industrie peut-être un frein à la diffusion de certaines normes. L'industrie géospatiale, y compris les fournisseurs de données géospatiales, peut être lente à offrir son soutien à des normes volontaires si elle estime qu'il y a de meilleures chances d'atteindre des objectifs et des résultats similaires avec une solution propriétaire. Ce point de vue est renforcé par la croyance populaire selon laquelle l'industrie peut développer et mettre sur le marché une solution propriétaire plus rapidement et mieux que ne le ferait une approche plus lente, fondée sur le consensus. Certains acteurs de l'industrie géospatiale sont également convaincus que « les normes se vendent en gros » en d'autres termes, pour établir efficacement une norme de facto, une entreprise n'a qu'à établir sa domination sur le marché.

Pour que les acteurs du marché acceptent d'adopter une norme, il faut avant tout que l'intérêt d'adopter cette norme soit correctement perçu par ces acteurs. Des cultures et habitudes internes existent au sein de toute grande organisation. Ces cultures peuvent résister à l'adoption de normes imposées par une agence ou une politique externe, soit parce que les normes ne répondent pas à leurs besoins commerciaux, soit parce que le coût de la conformité et du respect des normes est trop élevé. Il existe une perception répandue au sein des industries selon laquelle un organisme qui modifie ses équipements ou son fonctionnement pour soutenir une norme supportera le coût total et ne récoltera aucun bénéfice. En réalité, ces organismes, généralement des agences gouvernementales, comblent une lacune là où les marchés n'ont pas réussi à fournir ces biens. Une gestion adéquate doit également être en place pour assurer le succès de toute mise en œuvre de normes. Sans une direction efficace, peu d'organisations seront prêtes à changer leur statu quo ou à prendre conscience des avantages de la normalisation.

Enfin, encore aujourd'hui, la méconnaissance globale du mécanisme de production des normes freine la participation de nombreuses entreprises ou organismes qui y auraient pourtant un intérêt. De nombreux utilisateurs et organismes de la communauté géospatiale conviennent, du moins en théorie, que les normes sont importantes ou du moins nécessaires. Cependant, leur niveau de sensibilisation aux organismes d'élaboration de normes, leur compréhension du processus d'établissement de normes et leur compréhension de la façon de planifier et de mettre en œuvre des normes sont faibles. Par

conséquent, la participation des organisations locales, étatiques, ou privés aux activités de normalisation nationale est souvent faible.

Avec la généralisation de la production des données géographiques au format numérique, la protection des données apparaît également comme un enjeu majeur de leur diffusion. La normalisation des données, si elle se concentre avant tout sur l'interopérabilité et la transmission des données, doit également se pencher sur les problèmes de cybersécurité associés à ces données numériques. Ces enjeux de cybersécurité concernent à la fois les systèmes d'informations géographiques civils et militaires.

2.3 Cybersécurité et normalisation des données géographiques, des enjeux transverses aux domaines civil et militaire

À l'heure où interconnexion et numérisation sont les maîtres mots de l'échange d'informations de toute nature, la cybersécurité devient un sujet de premier plan également dans le domaine des informations géographiques. Depuis la fin des années 1990 et les avancées en matière de production de données géographiques numériques, ce mode de diffusion est devenu de loin le mode prioritaire de partage de ces données. Cette nouvelle réalité entraîne dans son sillage la nécessité de renforcer la protection de ces données, maintenant principalement diffusées et stockées par le biais de réseaux informatiques. Cela fait donc rentrer la géographie dans le domaine de la cybersécurité et fait des données géographiques de potentielles cibles pour des attaques cyber, à des fins de demande de rançons ou de destruction de ces données. Si la compétition internationale en matière de technologie n'est pas nouvelle, contrairement à l'ère industrielle, à l'ère numérique, elle ne porte pas seulement sur le nombre de chars, de navires, d'avions et de brigades, mais aussi sur le contrôle des réseaux, des plateformes et des logiciels[159]. Cela représente une transformation importante, l'établissement de normes dans ces domaines techniques aura des retombées géopolitiques importantes. Comme expliqué précédemment, au vu du rôle stratégique que remplissent ces données, à la fois dans le domaine civil et militaire, les protéger doit constituer une priorité de tous les instants pour l'ensemble des acteurs impliqués dans leur production et leur gestion.

Face à ce besoin de renforcement des enjeux liés aux attaques cyber au sein des acteurs de la géographie, la normalisation de ces données à également un rôle à jouer. En effet, la diffusion de

[159] Beckley M., « China's century? Why America's edge will endure », in *International Security*, Vol.36, N°3, pp.41-78, Hiver 2011/12.

normes ouvertes incluant des recommandations à des fins de protection des données contribue également à renforcer les mesures de cybersécurité qui peuvent être prises. Ainsi, la participation aux travaux de normalisation permet de réduire le risque de voir émerger des normes internationales préjudiciables à la sécurité et à la souveraineté numérique. De fait, les normes, une fois adoptées, étant reprises par les acteurs privés et publics, dans la conception de leurs produits et spécifications techniques, elles participent directement à façonner l'environnement cyber international. À titre d'exemple, la révision récente des critères communs en matière de cybersécurité à l'ISO[160] a vu les acteurs américains et anglais proposer d'adopter une démarche d'évaluation de la cybersécurité reposant essentiellement sur la conformité. Cette approche diverge de celle, plus exigeante, appliquée en France par les CESTI[161] [162]. La démarche favorisée par la France a pu être préservée dans la norme finale par la participation des experts français et allemands aux différentes étapes de préparation de la norme. Cependant, encore aujourd'hui, un long chemin reste à parcourir avant que la cybersécurité soit autant associée à la production des données géographique qu'elle le devrait, au regard de l'omniprésence du numérique dans les processus de production de ces données. De plus, le cyberespace est de plus en plus marqué par l'émergence de rivalités géopolitiques, particulièrement depuis l'invasion de l'Ukraine par la Russie le 24 février 2022, qui a accéléré l'emploi des cyberattaques par des acteurs étatiques ou affiliés à ces derniers, des acteurs autrefois en retrait par rapport à l'omniprésence des organisations criminelles et autres hackers cherchant des gains financiers, bien que ces derniers constituent toujours la majorité des attaques enregistrées ces dernières années[163]. De par l'importante diffusion des informations géographiques, l'omniprésence du numérique, ainsi que l'aggravation des tensions géopolitiques sur la scène internationale et le retour de la guerre conventionnelle sur le continent européen, il apparaît plus que nécessaire pour la France, ainsi que ses alliées de renforcer leurs capacités de protection de leurs données géographiques. Ces dernières peuvent en effet être l'objet d'attaques cyber à tout moment, et ce, qu'elles soient employées à des fins civiles ou militaires. Dans cette lutte de tous les instants qu'est la protection des données contre de potentielles attaques cyber, le processus de normalisation, à toutes les échelles, peut jouer un rôle crucial pour renforcer la sécurité de nos données, et participer à la construction d'un monde plus sûr. Avant de nous pencher sur les raisons qui font de la normalisation une étape essentielle de la protection

---

160 La norme ISO/IEC 15408 Sécurités de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information, encadre l'évaluation de cybersécurité des solutions numériques.

161 Centre d'évaluation de la sécurité des technologies de l'information.

162 La solution proposée par les Américains et les Anglais vise avant tout à vérifier que le produit répond aux exigences et que le développement soit correct, en suivant des tests normalisés. Là où, en France les testeurs sont encouragés à suivre leurs propres tests, afin de mener plus avant le niveau de sécurité du produit.

163 PwC, « Cyber Threats 2022: A Year in Retrospect », 2023. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html

des données géographiques, il est essentiel de comprendre quels sont les acteurs impliqués dans la protection de ces données et l'importance de la menace cyber pour les données géographiques.

Le numérique est omniprésent dans nos sociétés, et représente un facteur de danger permanent pour les individus, l'État et les sociétés privés. Les rançongiciels, ou *ransomwares*, constituent aujourd'hui la principale menace, pour les administrations comme les individus[164]. Si la plupart des attaques de ce type concernent des mails frauduleux envoyés à des individus et ne représentent pas de danger pour la sécurité nationale, elles représentent une menace constante pour les citoyens français. Les attaques cybers représentent une menace souvent sous-estimée, mais particulièrement importante pour les gestionnaires de données géographiques, en particulier au sein d'administrations territoriales, qui font face au risque de manipulation ou de destruction des données produites et gérées par les collectivités. Ainsi, certains groupes cybercriminels très organisés pénètrent les réseaux de leurs victimes, chiffrent des données pour les rendre inaccessibles afin d'exiger des rançons dont le montant va croissant et se chiffre parfois en millions d'euros. En France, le développement de la plateforme cybermalveillance.gouv.fr, fondée le 3 mars 2017[165], permet de diffuser des conseils élémentaires, mais indispensables et met à disposition tout un écosystème de prestataires privés à même d'aider les potentielles victimes.

Bien plus dangereuses sont les attaques lancées par les États ou des groupes de hackers organisés, souvent soupçonnés d'être affiliées à des États. Le risque d'espionnage de nos activités par l'infiltration de nos réseaux informatiques demeure une menace constante. Ainsi, dans le cas des informations géographiques, le sabotage de nos systèmes d'informations géographiques nationaux sur Internet peut avoir de lourdes conséquences sur la poursuite de projet d'aménagement du territoire à tous les échelons territoriaux. Dans ce domaine, il est important de reconnaître que nous n'avons pas d'alliés incontestables, et que le risque d'espionnage peut émaner aussi bien d'États hostiles à nos intérêts que de nos propres alliés. La nature complexe des relations internationales et des enjeux géopolitiques implique une vigilance constante pour protéger la sécurité et la confidentialité de nos informations sensibles. Les attaques cyber et l'espionnage informatique peuvent provenir de diverses sources, nécessitant ainsi une approche proactive en matière de sécurité numérique pour prévenir et contrer de telles menaces, indépendamment de l'origine potentielle des attaquants. Des questions de souveraineté interviennent dans notre capacité à gérer des données et à faire face à ce type de crises. Face à cette réalité, l'État et des industriels français et européens ont décidé de coopérer pour

---

[164] Assemblée Nationale, « Compte rendu Commission de la défense nationale et des forces armées — Audition, à huis clos, de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information. », Compte rendu n° 54, 27 mai 2020.

[165] Site officiel de la plateforme cybermalveillance.gouv.fr https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/qui-sommes-nous

développer des systèmes capables de traiter massivement des données sans dépendre systématiquement d'entreprises américaines. Cette démarche vise à renforcer l'autonomie et la maîtrise des technologies utilisées dans le traitement des données, réduisant ainsi la dépendance envers des acteurs étrangers et préservant la souveraineté nationale et européenne dans ce domaine stratégique. Ces collaborations visent à assurer une gestion plus indépendante et sécurisée des données, tout en favorisant le développement de solutions innovantes au niveau national et européen. De plus, plusieurs acteurs industriels d'importances ont démontré leur capacité à travailler avec le ministère des armées et la direction générale de l'armement (DGA), acteurs auxquels seul s'applique le droit français et européen.

L'industrie de l'armement, l'industrie spatiale et la BITD sont ciblées par de l'espionnage de haut niveau. La récente attaque informatique ayant visé Airbus en 2019 montre ainsi la nécessité de sécuriser l'ensemble de l'écosystème[166]. Une attaque particulièrement préoccupante au vu de l'importance du groupement Thales-Airbus dans les activités de la défense liées à la production de données géographiques. Depuis longtemps les industriels ne fonctionnent plus de façon isolée, mais plutôt au sein d'un écosystème dense et varié, impliquant des PME, de grands groupes, voire des acteurs étrangers. Cette interconnexion augmente fortement la surface d'attaque pour des attaquants potentiels, qui adoptent souvent la stratégie de cibler les sous-traitants afin de remonter au cœur des réseaux de leur cible en exploitant des accès légitimes. Cela souligne l'importance de la sécurité de l'ensemble de la chaîne d'approvisionnement et la nécessité pour les entreprises, grandes et petites, de mettre en place des mesures de cybersécurité robustes. Les attaques visant les sous-traitants peuvent avoir des implications graves, car elles peuvent fournir aux cybercriminels un accès privilégié aux réseaux et aux données sensibles de l'entreprise principale. La sensibilisation, la collaboration et la mise en place de protocoles de sécurité efficaces tout au long de la chaîne d'approvisionnement sont essentielles pour contrer ces menaces et renforcer la résilience globale du système. Dès 2013, la France a été le premier pays au monde à adopter une réglementation stricte sur la sécurité des opérateurs d'importance vitale[167]. Une initiative qui a permis de renforcer la prise en compte de la cybersécurité dans l'industrie de l'armement et d'autres secteurs, comme l'énergie, les transports ou les télécoms, jugés critiques pour la sécurité nationale.

Les enjeux liés à la cybersécurité et à la production de données géographiques sont intrinsèquement liés pour la France, qui doit veiller à préserver sa souveraineté. Les États membres de l'UE et la Commission européenne jouent un rôle crucial dans la lutte contre les menaces cyber, tout comme nos partenaires internationaux les plus proches, dans la protection et l'échange d'informations

[166] https://www.lemondeinformatique.fr/actualites/lire-altran-et-airbus-pirates-l-heure-des-cyberattaques-de-masse-a-t-elle-sonne-74185.html

[167] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

géographiques. La nécessité de concilier la souveraineté nationale avec une autonomie stratégique européenne est primordiale. Il est crucial de ne pas opposer la souveraineté européenne et la souveraineté nationale, car elles se complètent mutuellement. Ces questions font l'objet de nombreuses discussions au sein de l'Union via l'ENISA[168]. La coopération au niveau européen est essentielle pour garantir une cybersécurité efficace, et l'Europe, en retour, a besoin notamment de la France et de l'Allemagne pour développer ces capacités à l'échelle européenne. Il est impératif que chaque État développe ses capacités cyber, tout en travaillant en réseau avec d'autres. La collaboration, soutenue par une volonté politique forte, est indispensable à la construction d'une autonomie stratégique européenne dans le domaine de la cybersécurité. De fait, l'échelon européen reste pour la France et l'ensemble des membres de l'Union une échelle cruciale dans le développement de normes en matière de cybersécurité comme géographiques.

Ainsi, dès 2016 avec la mise en place de la directive « Network and Information Security » (NIS)[169], transposé au niveau national en 2018, l'Union européenne avait amorcé la mise en place d'une cybersécurité partagée à l'échelle européenne, en augmentant le niveau de cybersécurité des acteurs majeurs de dix secteurs d'activités (représentant environ une centaine d'entités en France). La directive NIS a ainsi obligé ces acteurs à déclarer leurs incidents de cybersécurité à leurs agences nationales compétentes (l'ANSSI en France), et à appliquer les mesures de sécurité nécessaires pour réduire l'exposition de leurs systèmes les plus critiques aux attaques cyber. Entrée en vigueur en janvier 2023, la directive européenne NIS2[170] est beaucoup plus ambitieuse que la précédente, en obligeant par exemple des milliers d'entreprises à renforcer leurs normes en matière de cybersécurité dans les domaines de l'administration publique, des télécommunications, des plateformes de réseaux sociaux, des services postaux, ou encore du secteur spatial. Cette nouvelle directive vise également à corriger de nombreuses irrégularités dans la mise en œuvre de la précédente au sein des différents États membres. Ainsi, la directive NIS2 s'étend aux entreprises privées. Plusieurs milliers d'entreprises de toutes tailles, des PME aux groupes du CAC40, seront amenées à se conformer à cette directive[171]. En effet, l'extrême interconnexion du marché européen implique qu'une mise en place incomplète des mesures de cybersécurité entraîne inévitablement un danger pour d'autres États membres. L'Europe passe ainsi d'une première phase plus passive, ouverte avec NIS1 consistant à avant tout à partager les informations en matière de cybersécurité entre les États membres, à une deuxième étape, plus active

---

168 European Union Agency for Cybersecurity (ENISA) : l'agence européenne pour la cybersécurité.

169 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

170 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

171 Myriam Quéméner, « Écosystème numérique : enjeux et défis pour les décideurs », S&D Magazine, n° 58, septembre 2023.

pour mettre en place des actions concrètes avant même que les attaques cyber n'aient lieu. La directive NIS2 vise a contrer l'explosion des attaques cyber dans tous les domaines, en élargissant le champ des entités considérées comme critiques et en les obligeant à prendre de meilleures mesures en matière de cybersécurité. Cette directive permet également de donner un cadre formel au réseau CyCLONe[172] qui rassemble l'ensemble des agences en charge de la cybersécurité des États membres. Ce dernier a été mis en place afin de contribuer à la mise en œuvre du plan d'action non contraignant de réponse en cas d'incident ou de crise informatique transfrontalière de la Commission européenne. L'ensemble des pays membres de l'Union devront retranscrire cette directive dans leur législation nationale d'ici à 2024. De plus, cette nouvelle législation connaît des retombés au-delà des frontières de l'Union européenne, en février 2023, l'Inde a ainsi fait passer une législation similaire à NIS2. Le parlement ukrainien a également travaillé à l'implémentation de NIS2 afin de lutter contre les attaques cyber massives lancées contre elle par la Russie depuis 2014.

Les mesures législatives européennes ne s'arrêtent pas là. Ainsi, trois règlements européens adoptés en 2022 portent sur la régulation de l'espace numérique européen. Le règlement sur les services numériques (DSA)[173], le règlement sur les marchés numériques (DMA)[174], et celui sur la gouvernance des données (DGA)[175]. Ces trois textes visent à organiser les relations entre les autorités nationales et leur participation aux travaux du comité européen pour les services numériques. Ainsi, en France l'ARCOM[176] a été désigné comme coordinateur des services numériques. L'exploitation et la protection des données numériques sont également au cœur des nouvelles législations européennes en matière de cybersécurité. Si le DGA est entré en vigueur le 24 septembre 2023 (cf. Figure 6), le Data Act[177] lui a été adopté en mars 2023. Ces deux textes visent à renforcer la compétitivité et la souveraineté de l'UE. Ils doivent permettre de définir un cadre harmonisé permettant aux acteurs économiques des pays membres de l'UE de tirer parti du potentiel des données et de favoriser l'innovation, le tout dans le respect du Règlement général sur la protection des données (RGPD)[178]. L'un des principaux objectifs du DGA est d'encourager à la réutilisation des données au sein des

---

172 Communiqué de presse ANSSI, « Blue OLEx 2020 : les États membres de l'Union européenne lancent le cyber Crisis Liaison Organisation Network (cyclone) », Paris, 29 septembre 2020.

173 Règlement (UE) 2022/2065 du parlement européen et du conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

174 Règlement (UE) 2022/1925 du parlement européen et du conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques).

175 Règlement (UE) 2022/868 du parlement européen et du conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données).

176 Autorité de régulation de la communication audiovisuelle et numérique (ARCOM).

177 Règlement du parlement européen et du conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), COM (2022) 68 finals, Bruxelles, 23 février 2022.

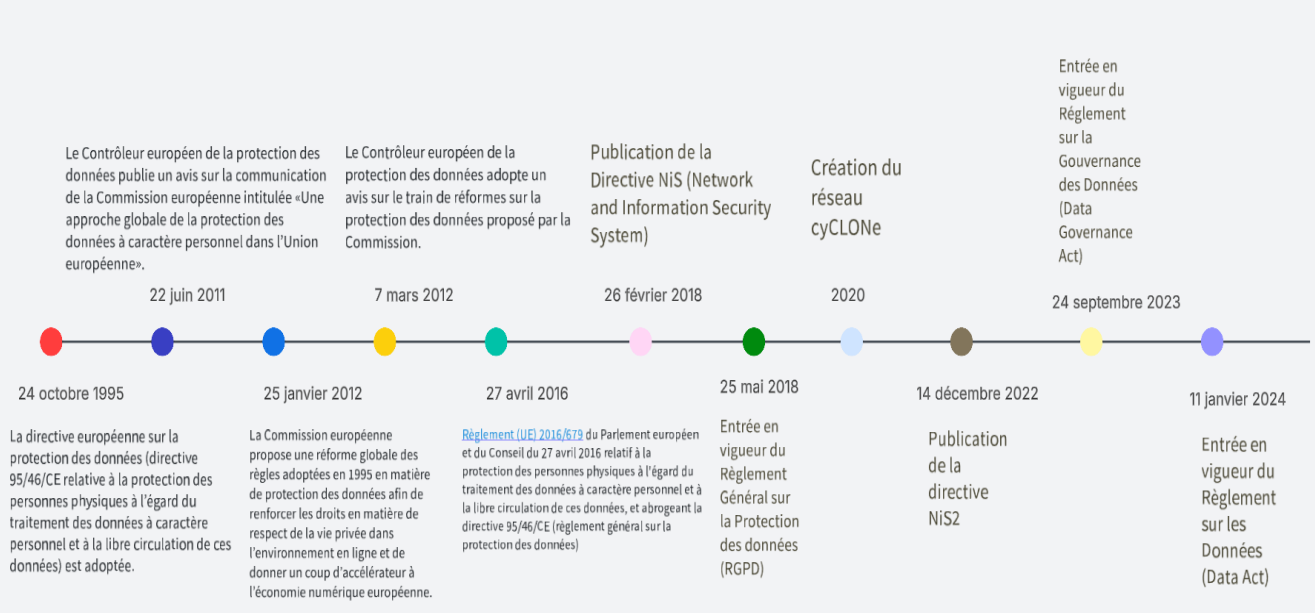
178 Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

organismes du secteur public, et proposer un cadre pour améliorer la disponibilité des données. Le DGA prévoit également la réutilisation des données du secteur public par des entreprises privées, y compris celles *« à caractère protégée »*[179]. Cependant ces dernières devront avoir été expurgées de leurs données personnelles avant réutilisation. Ce projet s'inscrit dans la continuité des travaux antérieurs, et complète la directive européenne de 2019 sur les données ouvertes[180], centré sur la réutilisation des données. En effet, le partage des données n'est pas toujours une évidence par les acteurs, autant d'obstacles que l'on rencontre également dans le domaine de la production de données géographiques. Le Data Act prévoit également la mise à disposition davantage de données auprès des acteurs économiques de l'UE. L'objectif étant de lever les obstacles juridiques, économiques et techniques à l'origine d'une sous-utilisation des données. Un des points d'intérêt du Data Act tient également dans le fait qu'il doit favoriser le changement de fournisseur de service cloud. La technologie cloud est de plus en plus utilisée pour stocker les données géographiques numériques très souvent extrêmement volumineuses. Ainsi, le choix d'un fournisseur cloud peut être lourd de conséquences en matière de protection de ces données et de leur confidentialité. De plus, certains fournisseurs de service cloud bloquent la possibilité de changer de fournisseur derrière de nombreuses contraintes financières et techniques visant à dissuader leur client d'en changer. Le Data Act cherche à modifier cela. Ainsi, il prévoit la suppression totale des, frais de sortie des données et des frais de changement de fournisseur trois ans après son entrée en vigueur (article 25). Le Data Act prévoit également de mettre à disposition des entités publiques des données détenues par des acteurs privés en cas de besoins exceptionnels, pour répondre à une situation d'urgence ou pour accomplir une mission d'intérêt public qui requitterait des données uniquement accessibles à cette société privée. Si cette législation entre en vigueur, de telles mesures pourraient grandement améliorer la diffusion et l'exploitation de données géographiques aujourd'hui détenues par des entités privées parfois peu enclines à partager leurs données.

[179] Garance Mathias, « Le marché unique des données : quels sont les apports du DGA et du Data Act ? », S&D Magazine, n° 58, septembre 2023.

[180] Directive (UE) 2019/1024 du parlement européen et du conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte).

Figure 6 : Évolutions de la législation européenne concernant la protection des données et la cybersécurité.



Source : *Union Européenne (2024)*

Ainsi, la souveraineté technologique ne réside pas dans la réalisation intégrale de tous les composants par soi-même, pas plus que le souci de préserver notre souveraineté ne doit s'accompagner d'un isolationnisme. Ainsi, dans le domaine militaire, la DGA n'assemble pas des systèmes d'armes composés exclusivement de composants français. Au contraire, la souveraineté technologique consiste à concevoir une architecture robuste et maîtrisée, puis à identifier parmi les différentes composantes, celles qui doivent être développées en interne par la Base industrielle et Technologique de la Défense (BITD), et celles qui peuvent être acquises sur étagère. La véritable difficulté réside dans la conception d'une architecture qui garantit un niveau de maîtrise suffisant. La sécurité élevée de nos systèmes d'armes demeure une priorité du ministère des armées et de la DGA. Les militaires ont été parmi les premiers en France à reconnaître l'importance de la menace cyber qui pèse sur leur chaîne d'approvisionnement et ont rapidement mis en place des structures pour y faire face. La gestion minutieuse de la conception, du développement et de l'acquisition des composants technologiques est cruciale pour garantir la sécurité et la souveraineté nationales dans le domaine militaire. Ce sont également les militaires qui aujourd'hui, saisissent le mieux l'importance des données géographiques et

de leur protection[181]. De fait, la BITD s'attelle au traitement de la question du cyber depuis environ une décennie. Les grands industriels de l'armement ont également fait des progrès constants dans le domaine de la cybersécurité au cours de cette période. Ainsi, le développement rapide des informations géographiques numériques s'est accompagné d'une mise en réseau de nombreux systèmes d'armes, ce qui ajoute une dimension supplémentaire aux défis en matière de sécurité. La protection des informations géographiques numériques, qui sont souvent essentielles pour les opérations militaires, nécessite une vigilance constante et une adaptation continue aux évolutions technologiques et aux menaces émergentes.

Surnommé « Network Centric Warfare »[182] par les Américains, concept désigné sous le nom de numérisation de l'espace de bataille (NEB) en France, cette nouvelle vision du commandement des opérations s'appuie sur la mise en réseau de l'ensemble des données géographiques pour l'ensemble des acteurs. Avec l'émergence du concept de numérisation de l'espace de bataille dans les années 1990, l'interconnexion homme-machine et la production de données géographiques numériques ont été placées au centre des développements technologiques dans les armées. L'armée française développe à partir de 1999 le concept de « bulle aéroterrestre », qui vise à maximiser l'interconnexion entre les différentes branches des forces armées et entre différentes armées alliées lors d'un engagement en coalition. Cela suppose la mise au point d'un réseau d'échange d'information, sous la forme d'un intranet tactique. Ce concept a aujourd'hui évolué avec l'émergence du cloud tactique, au cœur de l'architecture du SCAF[183]. Ce dernier vise à pousser l'interconnexion des réseaux numériques jusque dans le cockpit des aviateurs, en s'appuyant sur les avancées en matière de technologies cloud. Si une telle solution offre des perspectives intéressantes en matière d'efficacité et de résilience de la puissance aérienne, cela à également pour conséquence d'augmenter la surface d'attaque et le risque cyber des systèmes d'armes[184]. Une attaque cyber réussie sur de tels systèmes pourrait ainsi provoquer de grave dysfonctionnement de l'appareil ou rendre indisponibles certains systèmes, notamment de localisation, dans des situations critiques. Ces évolutions soulignent également la nécessité du développement des normes, nécessaires au partage d'informations, notamment géographiques, qui constituent une condition sine qua non de la mise en place du cloud tactique. Divers systèmes d'information ont été conçus pour mettre au service des différentes armes les bénéfices de la numérisation du champ de

---

181 Capo-Canellas Vincent, « Rapport d'information fait au nom de la commission des finances sur l'Institut national de l'information géographique et forestières (IGN) », n° 17, Sénat, 5 octobre 2022.

182 Cebrowski Arthur K., « Network-Centric Warfare : Its Origin and Future », US Naval Institute Proceedings, janvier 1998.

183 Le système de combat aérien du futur (SCAF) désigne un projet européen d'un ensemble de systèmes d'armes aériens interconnectés impliquant la France, l'Allemagne, l'Espagne et la Belgique (en tant qu'observateur).

184 Gros Philippe, « Le "cloud tactique", un élément essentiel du système de combat aérien du futur », Fondation pour la Recherche scientifique, note n° 8/19, 19 juin 2019.

bataille également dans l'armée de Terre. Ainsi, le système Atlas-canon, entré en service en 2004[185] afin de remplacer le système automatisé de transmission Atila datant des années 1970. Il permet l'automatisation des tirs et de l'acquisition des cibles, grâce à un système d'information et de communication interopérable avec les autres armes et les nations alliées. En effet, le système Atlas est intégré au sein de l'ASCA (Artillery System Cooperation Activities), un programme d'interopérabilité dédié à l'artillerie au sein de l'OTAN. Un tel système repose sur l'acquisition et l'exploitation de données géographiques et météorologiques d'une grande précision et diffusable par le biais de ce système d'information, au cœur duquel se situent les outils de géolocalisation et de visualisation cartographique. La production de modèles numériques de terrain (MNT) en 3D, ou encore d'orthoimages permettant un géoréférencement précis, sont intégrés dans des systèmes d'armes présents dans toutes les branches des forces armées, ainsi que dans des programmes interarmées, comme le programme GEODE 4D, permettant une fusion de données optimale pour l'ensemble des acteurs.

La visualisation en temps réel du mouvement des unités alliées, et ennemis identifiés grâce à la technologie GPS et la visualisation cartographique permet de dissiper une partie du brouillard de guerre et renforce les capacités de manœuvre et la réactivité des unités sur le champ de bataille. Cette mise en réseau des combattants et des informations s'appuie sur la collecte, le traitement, l'analyse et la diffusion en temps réel des informations disponibles à tous les échelons de commandement par le biais d'outils de visualisations et de capteurs mobiles intégrés à un système d'information unique. Les exercices en coalition, tels que CWIX (Coalition Warrior Interoperability Exploration, Experimentation, Examination Exercise)[186] au sein de l'OTAN développent également l'interopérabilité des réseaux afin de ne pas perdre les avantages acquis par le développement de ces systèmes d'information nationale pendant les opérations interalliées. De nouveau les besoins en termes d'interopérabilité sont importants et la normalisation des réseaux, des données employées en passant par les protocoles d'échange et d'affichage des données, est au cœur du développement de la NEB. Dans le domaine de la lutte contre les cyberattaques, les exercices Locked Shields menés par l'OTAN visent également à entraîner directement les experts en sécurité des membres de l'Alliance à faire face à des attaques cyber. Ces exercices visent à entraîner les nations membres à défendre leurs réseaux, mais également à communiquer en cas de crise et à évaluer les critères juridiques afin de pouvoir qualifier la nature des attaques subies et les actions à prendre en conséquence.

---

185 « Du célèbre canon de 75 à la révolution de l'information », in *European Security*, 1er août 2006.

186 La Coalition Warrior Interoperability Exercise est un exercice annuel des membres de l'OTAN visant à tester l'interopérabilité des systèmes d'armes et à garantir la mise en réseau efficace des armées des membres de l'alliance atlantique.

Cependant, la mise en application de la NEB fait face à de nombreuses limites. Tout d'abord les coûts liés au développement des programmes sont extrêmement élevés et repoussent souvent l'achèvement des programmes en question. Le programme GEODE 4D, qui vise à développer un système d'information centralisé regroupant l'ensemble des informations géographiques et météorologiques disponibles pour toutes les armes sur les théâtres d'opérations où sont déployés les armées, est un bon exemple, ce dernier est développé depuis plusieurs années et connaît de nombreuses évolutions pour garder son système à jour face au développement technologique très rapide dans le domaine, le rendant difficile à exploiter pour les opérationnels. La surcharge technologique pose également problème, en nécessitant des systèmes toujours plus performants et capables d'emmagasiner des charges de données toujours plus importantes, entraînant une explosion des coûts de fonctionnement et de maintenance. La multiplication des systèmes d'information au sein des différentes branches des forces armées rend également leur normalisation difficile.

Enfin, il faut garder à l'esprit que la mise en réseau des informations rend immédiatement vulnérables ces systèmes d'information aux attaques informatiques. La guerre en Ukraine a démontré l'usage expansif fait par les différents belligérants des outils de brouillage et des attaques cyber destinées à perturber les systèmes d'information adverses à tous les échelons[187]. En France, le développement du programme « Scorpion »[188] visant à l'interconnexion l'ensemble des groupements tactiques interarmes (GTIA) avec l'ensemble des intervenants de la bulle aéroterrestre autour d'un système d'information commun et fédérateur, le système d'information du combat Scorpion (SICS), nécessite des audits de cybersécurités constants afin de s'assurer de la sûreté des informations transmises. Cependant, des règles de cybersécurité trop encombrantes pour les utilisateurs menacent de rendre le SICS difficile d'emploi. Les problèmes de cybersécurité associés au développement de ces systèmes d'information doivent être au cœur du développement des informations géographiques, car ces dernières peuvent faire office de porte d'entrée pour un cyberattaquant au sein d'un système d'information. L'acculturation à la donnée géographique numérique des utilisateurs finaux peut également poser problème, notamment en sous-exploitant les informations vectrices qui permettent de disséminer un grand nombre d'informations complémentaires sur les éléments physiques de la carte, et qui ne sont pas toujours interrogées par les soldats sur le terrain. Le domaine maritime est particulièrement à risque, du fait de l'hyper centralisation des systèmes électroniques embarqués au sein des navires[189]. De fait, l'interconnexion entre systèmes physiques et électroniques nécessaire au fonctionnement d'un navire moderne entraîne une augmentation sans précédent de la surface d'attaque,

[187] Thibault Fouillet, « Quelle place pour le cyber dans la manœuvre aéroterrestre ? », DEFTECH, n° 3, octobre-décembre 2022.

[188] Synergie du contact renforcée par la polyvalence et l'infovalorisation.

[189] Petit Claire, « Les enjeux de la cybersécurisation du milieu maritime », DEFTECH, n° 3, octobre-décembre 2022.

où une attaque cyber peut entraîner le dysfonctionnement de systèmes vitaux[190]. Ainsi, les cartes maritimes de navigation, aujourd'hui entièrement numérisées et distribuées par des acteurs privés divers, peuvent potentiellement subir des manipulations de la part d'attaquant aux conséquences désastreuses pour les navires infectés. En effet, une fois que le cyberattaquant s'est introduit au sein d'un navire par le biais de sa carte maritime, il pourra potentiellement poursuivre son attaque contre l'ensemble des systèmes du navire. De plus, avec le développement des navires autonomes entièrement connectés, le milieu maritime sera à l'avenir sujet à une augmentation importante du risque cyber qu'il est nécessaire d'anticiper a plus tôt[191]. Ce risque a poussé l'Organisation hydrographique internationale (IHO) à incorporer à sa nouvelle série de norme sur le modèle universel de données hydrographiques, la série S-100, dont la première partie a été publiée fin 2022[192], un chapitre entier (le chapitre 15) dédié aux mesures de chiffrement recommandées pour se conformer à cette nouvelle norme internationale. La norme S-100 est un document cadre destiné au développement de produits et services numériques pour les communautés hydrographiques, maritimes et SIG. Elle comprend plusieurs parties fondées sur les normes géospatiales élaborées par le Comité technique 211 (ISO/TC 211) de l'Organisation internationale de normalisation. La norme S-100 fournit une norme pour les données hydrographiques qui peut prendre en charge une grande variété de sources de données numériques liées à l'hydrographie, et qui est entièrement alignée sur les principales normes géographiques internationales, en particulier la série de normes géographiques ISO 19100. Cela garantie une intégration plus facile des données et des applications hydrographiques aux SIG. Le chapitre 15 spécifie les mécanismes, les structures et le contenu requis pour la mise en œuvre des protections contre la copie et/ou des méthodes d'authentification des produits S-100. Il définit des méthodes et des algorithmes normalisés pour le cryptage des composants de fichiers des ensembles de données ainsi que des catalogues d'objets et de représentations. Des algorithmes et des méthodes pour la production de signatures numériques sont définis, ainsi que l'infrastructure nécessaire à la gestion des clés et à l'assurance de l'identité dans le cadre du système de protection des données de l'IHO.

Parmi les acteurs concernés par l'augmentation du risque cyber, il est indéniable que les collectivités territoriales jouent un rôle majeur dans la gestion du risque cyber lié à la protection des données géographiques dans le milieu civil. Cependant, il est également vrai qu'elles semblent souvent mal préparées à faire face à ce risque croissant. Les attaques cyber dirigées contre ces collectivités

---

190 Pelissero Nicolas, Merino Laso Pedro et Puentes John. « Impact Assessment of Anomaly Propagation in a Naval Water Distribution Cyber-Physical System »., CSR 2021 : IEEE International Conference on Cyber Security and Resilience, Rhodes, juillet 2021.

191 Cho Sungbaek et al., « Cybersecurity Considerations in Autonomous Ships », NATO Cooperative Cyber Defense Center of Excellence (CCDCOE), Tallinn, 2022.

192 S-100 Universal Hydrographic Data Model. Accessible en anglais ici : https://iho.int/en/s-100-universal-hydrographic-data-model

peuvent avoir des conséquences graves sur la vie quotidienne et la sécurité des citoyens. Dans l'exercice de leurs compétences et dans leurs relations avec leurs administrés, les collectivités locales et leurs établissements publics sont tenus de respecter la réglementation relative aux données personnelles. Ces données sont nombreuses au sein des collectivités locales, qu'il s'agisse d'une utilisation interne (gestion des ressources humaines, vidéosurveillance, etc.) ou externe (État civil, listes électorales, inscriptions scolaires, etc.)[193]. Si les grandes entreprises disposent de moyen financier conséquent qu'elles peuvent mettre au service de leur protection cyber, il n'en est rien pour les PME, ainsi que beaucoup de collectivités territoriales. Ainsi, l'enquête menée en 2021 par les services de la plateforme cybermalveillance.gouv.fr auprès des communes de moins de 3 500 habitants a révélé que 65 % d'entre elles estimaient que le risque numérique était faible, voire inexistant, ou disaient ne pas savoir l'évalue r[194]. Depuis plusieurs années maintenant, la prise de conscience cyber a progressé, mais cela reste encore insuffisant.

Un des points importants concernant la cybersécurité que le cas des collectivités locales de petite et moyenne importance souligne bien, est la prise en compte de la nature constante du risque cyber pour tous les organismes traitant de données numériques. Beaucoup d'attention a été portée, à juste titre, aux opérateurs d'importance vitale (OIV) en France, afin de garantir un meilleur niveau de protection à ces derniers[195] [196]. Cependant il faut prendre garde à ce que les OIV ne deviennent pas l'arbre qui cache la forêt, empêchant d'anticiper des attaques sur des cibles en apparence moins sensibles, mais dont les conséquences pourraient également être grave, ou tout du moins coûteuses. Depuis le passage de la loi NOTRe[197] la région est devenue l'échelon territorial de référence pour la collecte et la gestion des informations géographiques sur le territoire. Les collectivités locales sont également amenées à gérer de plus en plus de données, et devienne des acteurs de premier plan de leur production, investissant parfois des sommes importantes pour la production de données géographiques sur leur territoire. Ces derrières étant des outils d'aide à la décision de plus en plus importante, nécessaire au développement d'un nombre croissant de projets et de politiques publiques, le manque de protection de ces données pourrait entraîner à terme des dysfonctionnements importants en cas d'attaque cyber sur ces infrastructures. De plus, l'argent investi dans ces projets serait perdu en cas de destruction totale des données.

Avec l'omniprésence du numérique dans nos sociétés contemporaines, et suite au développement de la géographie numérique en parallèle, les questions de cybersécurité sont devenues prégnantes pour

193 CNIL, « Guide obligations et responsabilités des collectivités locales en matière de cybersécurité », 2021.
194 *Ibid*
195 Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
196 Livre blanc sur la défense et la sécurité nationale 2013.
197 Loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République.

l'ensemble des acteurs et utilisateurs de la géographie à la fois dans le domaine civil et militaire. Face à un risque cyber désormais omniprésent, la normalisation, à la fois dans le domaine des données géographiques et celui des informations de la communication au sens large, à son rôle à jouer pour renforcer la cybersécurité internationale. La participation de la France au sein des organes internationaux de normalisation doit faire partie intégrale de la stratégie française en matière de cybersécurité en servant de tremplin à l'application de normes internationales dans ce domaine qui respecte les niveaux d'exigence attendus par les instances françaises en la matière. Qu'il s'agisse de protéger les données détenues par nos collectivités territoriales, autant que les réseaux d'information géospatiale mise en place par nos armées, le maintien de normes sécurisées en matière de production de données géographiques est un enjeu de premier plan pour la protection de notre souveraineté.

3. Les enjeux du processus normatif

Les très larges applications des données géographiques, et l'existence d'un marché international très actif autant au niveau de leur production proprement dite que de leur diffusion, font des données géographiques un domaine très actif en matière de normalisation. L'omniprésence de ces données comme outil d'aide à la décision à la fois au niveau civil et militaire fait des données géographiques des données d'une importance capitale, dont la maîtrise de la production et de la diffusion sont des enjeux de premier plan pour les États. En permettant l'interopérabilité des systèmes informatiques et des données, la normalisation joue un rôle crucial pour le développement des données géographiques et leur réutilisation, qui sont les conditions sine qua non de leur exploitation. Les enjeux de souveraineté liés à la maîtrise des données géographiques se retrouvent également dans leur normalisation qui cristallise ces enjeux. Ainsi, la compétition en matière de norme définit quel acteur, qu'il s'agisse de consortiums industriels ou d'États, sera en mesure de fournir avec le plus d'efficacité à ses clients ou à ses citoyens des produits dernier cri s'appuyant sur ces données, apportant aux acteurs les plus impliqués dans ces processus des avantages compétitifs de nature politique, économique et éthique.

3.1 Des enjeux politiques, économiques et éthiques

Comme indiqué précédemment, contrairement aux apparences, les normes sont loin d'être apolitiques. Comme souligné notamment par Tim Rühlig, elles ne se limitent pas à des discussions entre des ingénieurs de premier plan dans leur domaine, à la recherche de solutions efficaces à des défis communs pour assurer l'interopérabilité entre les systèmes et un certain niveau de sécurité : *« un*

examen plus approfondi révèle qu'elles peuvent être bien plus que des spécifications techniques »[198]. Les normes sont un de ces domaines peu connus et pourtant essentiels pour l'autonomie stratégique et la maîtrise de la souveraineté. En effet, le contrôle des normes techniques procure un avantage décisif dans le développement de nouvelles technologies et des futurs produits qui en dépendent. Rühlig propose notamment le concept de *« pouvoir de normalisation technique »* (technical standardisation), qui s'exerce selon lui dans quatre dimensions, économiques, juridique, polkitique et discursive[199]. Cette thèse théorise l'existence d'un véritable « Standard Power », qui peut se définir comme une sous-section du Soft Power s'appuyant sur le contrôle par les États des processus de normalisation afin de s'assurer divers avantages, dans le domaine économique, politique, juridique et éthique.

Tout d'abord, économiquement parlant, Rühlig rappelle que la maîtrise des normes assure aux sociétés privées un avantage considérable. Ainsi, une grande partie des normes techniques est constituée de technologies brevetées. Environ 55 % de toutes les normes des technologies de l'information et de la communication (TIC) sont des technologies brevetées largement appliquées dans des domaines tels que les télécommunications, l'électronique, le secteur de la santé, ou encore le secteur automobile. Un tiers de l'ensemble de la technologie sans fil de nouvelle génération, mieux connue sous le nom de 5G, serait constitué de technologies brevetées standardisées[200]. À première vue, cela peut surprendre, car les normes techniques et les brevets ont des objectifs opposés. Les brevets protègent les inventions et empêchent les concurrents d'utiliser les nouvelles inventions. Les normes techniques, en revanche, répartissent les solutions technologiques entre les fabricants afin de permettre leur interopérabilité et de garantir un niveau de sécurité fondamental. Cette contradiction est résolue par des systèmes de licences. Les détenteurs de brevets essentiels au respect d'une norme technique, appelés Brevets essentiels à la Norme (BEN), s'engagent à concéder une licence pour leur technologie brevetée à des conditions équitables, raisonnables et non discriminatoires (RAND). Bien que ce cadre garantisse que les BEN soient disponibles pour tous les fournisseurs et pas seulement pour le détenteur du brevet, des montants énormes de redevances doivent être versés aux inventeurs des technologies innovantes sous-jacentes aux BEN respectifs. Le géant suédois de la technologie, Ericsson, a par exemple gagné 5,2 milliards d'euros en octroyant des licences sur des technologies en 2017, ce qui représente plus de 20 % de son chiffre d'affaires[201]. De plus, les entreprises qui ne parviennent pas à faire de leurs solutions technologiques des normes techniques doivent revoir la conception de leurs

198 Rühlig Tim, « China, Europe and the New Power Competition over Technical Standards », UI Brief n°1, Stockholm, The Swedish Institute of international Affairs, 2021.

199 Ibid

200 Ibid

201 Filippo Gualtiero Blancato, "Regulate to Dominate: The Geopolitics of Standard-Setting in Digital Technologies and its Strategic Implications for the EU", UNU-CRIS Institute on Comparative Regional Integration Studies, Policy Brief n° 8, 2019.

produits pour se conformer aux normes qui génèrent l'interopérabilité. Il en résulte des coûts de changement ou d'adaptation qui affectent inévitablement leur compétitivité. Rühlig rappelle à ce propos l'expression prêtée à Werner von Siemens « celui qui possède les normes possède le marché ».

La dimension financière de la normalisation s'impose aussi dans la façon dont la normalisation internationale est organisée. Si la participation à un groupe de travail est généralement ouverte à n'importe quelle personne physique ou organisation intéressée, cela est rarement gratuit. Les sommes à verser pour pouvoir entrent dans un organisme de normalisation agréé varient énormément d'un organisme à l'autre et en fonction de la nature de celui qui cherche à y entrer (personne physique, société privée, laboratoire, etc.). Les consortiums privés sont également largement fondés sur le principe de « payer pour jouer » et incitent leurs participants à augmenter leur participation financière en échange d'une augmentation du nombre de représentants aux réunions. Un meilleur investissement financier permet également d'occuper des postes à responsabilité au sein des instances de gouvernance des consortiums et organisation internationales. Cette situation décourage de nombreuses PME à participer à ces processus de normalisation. Même l'ISO divise ses différents membres en fonction de leur participation financière, et seuls les pays capables de régler la note peuvent accéder au statut de nation participante. De plus, devenir une nation participante engendre certaines obligations, notamment celle d'accueillir dans un futur plus ou moins proche une des réunions plénières de l'ISO. S'il s'agit d'une source de prestige, qui démontre le poids politique et l'influence du pays capable d'accueillir les experts mondiaux dans ce domaine, cela engendre également des coûts très élevés, qui peuvent là encore pousser certaines nations à y réfléchir à deux fois avant de s'investir dans la normalisation mondiale.

De même, sur la scène internationale, les déplacements fréquents qui accompagnent nécessairement une participation active aux travaux de normalisation constituent un casse-tête constant pour les différents représentants nationaux. Là encore, la surreprésentation d'acteurs européens tend à concentrer les réunions plénières des différents comités techniques autour du Vieux Continent, engendrant de nombreuses frustrations parmi les participants non européens, en particulier parmi les pays en développement souvent réticents à dépenser les sommes engendrées par les déplacements de leurs représentants. Si la généralisation des réunions à distance rend plus aisée la participation des membres des comités qui n'ont pas pu se déplacer, cela reste une solution partielle. Non seulement le décalage horaire peut rendre impossible la participation de certains acteurs malgré l'existence de réunions virtuelles, mais, de l'aveu même de tous les participants à ces réunions, les travaux réalisés à distance sont beaucoup plus laborieux que lorsque l'ensemble des participants se rencontrent. Les rapports humains sont cruciaux dans la normalisation, où la recherche du consensus, qui implique nécessairement une négociation, est capitale. Par conséquent l'impossibilité de se déplacer peut

handicaper de façon disproportionnée certains acteurs. Indéniablement la normalisation est géographique et humaine, et les lieux de la normalisation dessinent des zones d'inclusion et d'exclusion évidente pour qui s'y penche suffisamment. Avec le développement de certains pays, ces lieux sont amenés à évoluer et les espaces européens ne sont plus systématiquement sélectionnés. À titre d'exemple, si la 55e réunion plénière de l'ISO/TC 211 a eu lieu à Stockholm en décembre 2022, la 56e a pris place à Jeonju en Corée du Sud en mai 2023, et la 57e s'est tenue à New Delhi en Inde en décembre 2023. Ces récents changements en matière de localisation des réunions plénières soulignent l'importance des acteurs asiatiques dans la normalisation des données géographiques qui deviennent des acteurs de premier plan. Ainsi, les développements technologiques démontrés par la Corée du Sud en matière de jumeaux numériques, une technologie en pleine expansion et dont la normalisation au sein du TC/211 ouvre de nombreuses opportunités en matière de développement économique et de gestion des risques, ont été au cœur des présentations sud-coréennes lors de la 55e réunion plénière de l'ISO/TC 211. De même, l'intérêt renforcé de l'Inde dans la gouvernance du TC/211 et de la normalisation des données géographiques n'est pas un hasard. Non seulement l'union indienne est soumise à des pressions environnementales de plus en plus fortes qui risquent de faire obstacle au développement de sa population, mais la défense de sa souveraineté dans l'océan indien est un sujet stratégique qui la pousse à s'intéresser de plus en plus étroitement aux projets portés par le TC/211 de l'ISO et l'IHO.

Le contrôle des normes a aussi des effets juridiques, en particulier concernant le respect des règles de l'Organisation mondiale du Commerce (OMC). Rühlig souligne ainsi que des normes volontaires deviennent, « par la porte dérobée » une composante du droit commercial international. En effet, un État dont les normes nationales s'écartent des normes internationales peut être jugé en infraction à l'accord de l'OMC sur les obstacles techniques au commerce, sauf à justifier cet écart par des exigences de santé, de sécurité ou de protection de l'environnement, ce qui n'est pas anodin dès lors qu'environ 80 % du commerce serait affecté par des normes et des règlements techniques[202]. Au niveau national, les normes techniques peuvent être référencées dans des documents juridiquement contraignants, le plus souvent dans des règlements. Par exemple, lorsque des règlements prescrivent certaines règles juridiquement contraignantes, les normes techniques peuvent servir de méthode pour faire respecter ces règles fixées dans ce règlement. Dans ce cas, les normes techniques restent volontaires sur le papier, mais prescrivent le moyen le plus simple pour les entreprises de garantir le respect de la réglementation juridiquement contraignante. Une situation qui peut devenir particulièrement difficile pour des entreprises étrangères qui cherchent à s'implanter sur un nouveau

[202] Rühligh Tim, « China, Europe and the New Power Competitoin over Technical Standards », UI Brief n°1, Stockholm, The Swedish Institute of internaitonal Affairs, 2021, p.5.

marché et qui se retrouvent à lutter avec des entreprises nationales déjà au fait de ces normes[203]. Des normes qui par ailleurs, peuvent obliger les sociétés à délivrer à l'État des informations jugées sensibles, ou à maintenir sur le territoire national l'intégralité des données produites par l'entreprise. Des règles draconiennes qui deviennent une façon détournée de faire du protectionnisme par certains États, en favorisant leurs sociétés nationales.

Sur le plan politique, l'adoption de certaines normes peut être un moyen pour certains États de faire pression sur d'autres, moins équipés dans ce domaine, afin de les pousser à l'adoption de normes techniques spécifiques. Les normes ne génèrent l'interopérabilité que dans le domaine où elles sont appliquées. Rühlig souligne ainsi également que les normes techniques peuvent créer des territoires technologiques séparés, de véritables *« enclaves technologiques »*[204] géographiquement séparées du reste du monde. À ce jour, par exemple, les normes techniques dans le secteur ferroviaire restent largement nationales ou régionales. Toutefois, si un pays A adopte les normes ferroviaires nationales d'un pays B, comme l'écartement des voies, l'entretien et la construction du chemin de fer ne peuvent être assurés que par des fournisseurs basés dans le pays B. Les autres fabricants produisent en utilisant des normes techniques incompatibles, leurs produits ne seraient tout simplement pas compatibles. Le pays A est donc verrouillé par la technologie du pays B et dépend entièrement des fournisseurs installés dans le pays B. Une situation rencontrée récemment par le Laos, qui a fait construire l'intégralité de sa nouvelle ligne de chemin de fer, achevée en décembre 2021, par la Chine, dans le cadre du programme des Nouvelles Routes de la Soie[205]. Le gouvernement chinois a pu imposer au Laos l'adoption exclusive des normes ferroviaires chinoises, rendant le pays entièrement dépendant aux experts techniques chinois pour l'entretien de son réseau ferroviaire. Les ramifications politiques d'une telle dépendance infrastructurelle sont difficiles à délimiter. Cependant, il y a fort à parier que le Laos y réfléchira à deux fois avant d'adopter une position divergente de celle de la Chine, sur quelque sujet politique que ce soit à l'avenir, au vu du risque non négligeable de se voir couper de sa seule ligne d'approvisionnement internationale.

Outre ces effets de verrouillage géographiques, Rühlig relève également que certains experts suggèrent que les normes techniques ont le potentiel d'empiéter sur « *ce qui est souvent considéré comme le joyau de la couronne du pouvoir étatique : la sécurité »*[206] . Certains observateurs font valoir que ceux qui développent une technologie sont susceptibles d'avoir une connaissance plus approfondie

---

203 Tim Rühlig, « The Shape of Things To Come : The Race to Control Technical Standardisation », The Swedish Institute of International Affairs and The European Union Chamber of Commerce in China, 2021.

204 Ibid, pp. 5 – 6

205 « China-Laos Railway builds on momentum in new year as cargo and passenger numbers grow », in *Global Times*, 8 février 2024.

206 Tim Rühlig, « The Shape of Things To Come : The Race to Control Technical Standardisation », The Swedish Institute of International Affairs and The European Union Chamber of Commerce in China, 2021, p.6.

de son fonctionnement, y compris de ses vulnérabilités. Une fois normalisée au niveau international, cette technologie se répand dans le monde entier. Lorsqu'il s'agit d'une infrastructure numérique critique, le développeur de la technologie en question possède une connaissance primordiale de ses failles qui peuvent être utilisées pour porter atteinte à la sécurité d'un adversaire[207]. Cependant relève Rühlig, d'autres observateurs font remarquer que la normalisation est un processus visant à la transparence maximale dans lequel il n'est guère possible de dissimuler les failles relatives à la sécurité aux yeux des ingénieurs d'adversaires potentiels. De ce point de vue, un degré élevé de normalisation augmente même la cybersécurité des produits concernés en assurant une transparence internationale. Quelle que soit la perspective la plus juste, la normalisation technique influence le degré de cybersécurité des technologies numériques critiques. Dans tous les cas, les normes techniques ont des implications politiques qui découlent des effets de verrouillage tout en affectant la cybersécurité des États[208].

La façon dont la technologie est conçue est hautement politique, car comme le rappelle Rühlig, *« la manière dont la technologie est conçue lui attribue des valeurs éthiques »*[209]. La technologie n'existe pas en vase clos, sans lien avec la politique. Les normes techniques sont importantes à cet égard, car elles formulent une « recette de base » en fixant les règles générales selon lesquelles les différents fabricants développent des produits spécifiques. Ainsi, les normes techniques façonnent ce qui est perçu comme une technologie « normale ». Rühlig en donne pour exemple le cas de la norme WAPI[210]. Aujourd'hui, par exemple, nous sommes habitués à ce que le Wi-Fi soit la norme dominante pour les réseaux locaux sans fil (WLAN). Toutefois, cela n'était pas du tout acquis. Quelques années après l'adoption du Wi-Fi comme norme internationale, la technologie concurrente WAPI a été proposée par la Chine comme nouvelle norme. [211] Elle promettait de meilleures performances, mais offrait une moins bonne protection de la vie privée que le Wi-Fi. WAPI a rencontré une résistance considérable et n'a finalement pas réussi à devenir une norme internationale, en grande partie à cause de problèmes de procédure. Que ce soit intentionnellement ou non, en rejetant WAPI, les organismes internationaux de normalisation ont privilégié la confidentialité par rapport aux performances, façonnant ainsi ce dont les consommateurs et les fabricants du monde entier peuvent attendre de la technologie WLAN. La normalisation constitue une source de pouvoir, car elle contribue à « normaliser » la technologie future, à y inscrire des valeurs politiques et éthiques et à renforcer l'image

---

207 Cooper A et al., Request for Comment (RFC) 6973: « Privacy Considerations for Internet Protocols », Internet Architecture Board, 2013. https://datatracker.ietf.org/doc/html/rfc6973

208 Rühligh Tim, « China, Europe and the New Power Competitoin over Technical Standards », UI Brief n°1, Stockholm, The Swedish Institute of internaitonal Affairs, 2021, p.6.

209 Ibid, p.7

210 Ibid, p7

211 Huawei et al., *New IP, «* Shaping Future Network: Propose to Initiate the Discussion of Strategy Transformation for ITU-T. Proposal to ITU-T TSAG », 2019. http://prod-upp-image-read.ft.com/ec34d7aa-70e6-11ea-95fe-fcd274e920ca

d'un État en tant que leader technologique[212] . À l'heure où la compétition internationale en matière de normalisation se renforce, la notion d'éthique est particulièrement importante, notamment pour les États européens qui défendent non seulement leur savoir-faire technologique sur la scène internationale, mais également *« les valeurs démocratiques fondamentales et les intérêts primordiaux de l'UE »* comme soulignée récemment par la nouvelle stratégie européenne sur la normalisation[213] . Cela est particulièrement important en ce qui concerne les normes harmonisées, adoptées sur la base de la législation d'harmonisation de l'Union et dont les références ont été publiées au Journal officiel de l'Union européenne, que la Cour de justice a considérées comme faisant partie du droit de l'Union aux fins de leur interprétation[214] . Ces dernières s'imposent donc à l'ensemble des membres de l'Union, et s'assurer qu'elles participent de la diffusion et du respect des valeurs de l'Union européenne est primordial. La normalisation technique peut être une source de pouvoir pour les États. Il n'est donc pas étonnant qu'elle soit devenue l'une des arènes les plus cruciales de la rivalité émergente entre puissances en matière de technologie. Les données géographiques n'échappent pas à ces questionnements. De plus, la numérisation des données géographiques, et plus globalement l'appartenance de l'Information géographique à la catégorie des Technologies de l'Information et de la Communication, fait que la normalisation des données géographiques tourne de plus en plus autour des évolutions technologiques permettant l'échange et la diffusion de ces données sur des supports numériques. La compétition internationale dans les domaines des technologies numériques, mais également spatiales, a un impact direct sur le débat en matière de normalisation de données géographiques. Comme en témoigne le lien étroit entre le développement de technologies spatiales et celui des normes concernant les données géographiques, telles quelles l'imagerie radar (SAR) ou laser (lidar).

3.2 Faut-il avoir peur de la Chine ?

Au cœur de la plupart des débats qui se tiennent ces dernières années concernant la dimension géopolitique de la normalisation, en particulier en occident, se trouve le retour en force de la RPC sur la scène internationale et ses possibles répercussions sur l'équilibre international de la normalisation, tous domaines confondus. Comme noté précédemment, la Chine reste aujourd'hui sous-représentée au sein des comités techniques de l'ISO, au vu de son poids économique, arrivant tout juste 6e en termes de

[212] Human Rights Council [HRC], Resolution A/HRC/RES/47/23: « New and Emerging Digital Technologies and Human Rights », 2021. https://undocs.org/Home/Mobile

[213] La Commission européenne, « Une stratégie de l'UE en matière de normalisation. Définir des normes mondiales à l'appui d'un marché unique européen résilient, vert et numérique », Bruxelles, 2 février 2022.

[214] Arrêt de la Cour de justice (troisième chambre) du 27 octobre 2016, C-613/14, ECLI : EU : C : 2016:821.

nombre de comités techniques, derrière des pays comme la France et le Royaume-Uni, pourtant bien moins important économiquement[215] . Cependant, malgré cette position toujours en demi-teinte, la progression chinoise en termes de participation au sein des instances internationales de normalisation n'en reste pas moins remarquable ces dernières années, une situation qui a attiré l'attention de nombreux observateurs internationaux, il reste cependant encore à déterminer si cette recrudescence chinoise en matière de normalisation représente un risque ou une opportunité pour la stratégie française dans ce domaine.

Le système actuel de gestion de la normalisation chinoise s'est principalement développé dans un contexte d'économie planifiée, qui prend ses racines dans la longue Histoire de la Chine impériale et qui s'est poursuivie avec l'émergence de la République populaire de Chine. Le système normatif chinois actuel est marqué par la fragmentation institutionnelle et la multiplicité des entités décisionnaires gouvernementale. Dans un premier temps, les mesures dirigistes en matière de normalisation se sont révélées très efficaces pour le rapide développement technologique de la Chine. La standardisation chinoise à l'époque contemporaine est marquée tout d'abord par une première période d'adoption massive de normes étrangères (1980-2000), usant des normes avant tous comme outils de transferts technologiques, afin de faire rattraper à la Chine son retard technologique sur l'occident[216] . Durant la période 2000-2010 marquée par la forte croissance de l'économie chinoise, la stratégie du gouvernement consistant à utiliser les normes pour encourager et promouvoir l'innovation locale a également été très efficace. En effet, le système de normalisation chinois fonctionne de façon multiscalaire malgré sa très forte centralisation, et laisse une large place dans certains domaines au développement régional des normes technologiques afin d'accommoder les énormes disparités régionales en matière de développement et de technologie. Une réalité qui accentue la grande complexité du système normatif chinois, et qui est souvent dénoncé par les observateurs étrangers[217] comme étant utilisée afin de faire de la concurrence déloyale aux entreprises étrangères cherchant à pénétrer le marché chinois. Quoi qu'on en pense, force est de constater que cette stratégie a été payante pour la Chine, qui a su s'appuyer sur une normalisation dirigiste à une période de leur histoire où leur industrie, certes déjà large, était composée de sociétés dont les capacités d'innovations n'étaient pas encore mûres pour rivaliser avec les sociétés européennes, américaines ou japonaises. Il faut également garder à l'esprit que la compétition internationale en matière de normalisation impose de « rattraper leur retard » aux entreprises issues des pays en développement, un processus qui peut être très difficile

---

215 AFNOR, B*aromètre international 2023*, 2023.

216 Wang Ping et Liang Zheng, « Beyond Government Control of China's Standardization System -- History, Current Status and Reform Suggestions », 27 janvier 2016

217 Kamensky Jack, « Standards Setting in China: Challenges and Best Practices »,The US-China Business Council, janvier 2020.

sans un fort soutien national à la normalisation locale et régionale, permettant de protéger ces entreprises et le marché dans lequel elles se développent face à la pénétration des sociétés étrangères venues de pays plus développés. Cependant, les années 2010-2015, marquées par un ralentissement de la croissance chinoise, ont mis en lumière de nombreux problèmes, notamment causés par le rôle excessif du gouvernement dans la normalisation et la multiplication des instances de gouvernance à tous les niveaux décisionnaires. Autant de facteurs considérés comme des entraves à l'innovation, à une période où la Chine cherche à diversifier son économie dans des domaines de pointe où les industries occidentales règnent en maître.

Aujourd'hui le système de normalisation chinois est toujours entièrement supervisé par le gouvernement, notamment par l'Agence de normalisation chinoise (Standardization Administration of China : SAC)[218] en charge de la normalisation nationale, par le biais des bureaux ou ministères relevant du Conseil d'État en charge de la normalisation sectorielle/ministérielle, ainsi que par les gouvernements locaux en charge de la normalisation locale. La normalisation locale concerne 22 provinces, 5 régions autonomes et 4 municipalités. Pour chaque gouvernement local, le bureau local de supervision technique est spécifiquement chargé de la normalisation dans cette région, tandis que la normalisation au niveau des préfectures, des districts et des comtés repose généralement sur l'institut local de normalisation et les associations locales de normalisation. Toutes les provinces et municipalités ont également leurs propres associations professionnelles de normalisation rassemblant diverses sociétés ou conglomérats industriels. Ces associations ne sont généralement pas des organisations réellement indépendantes et entretiennent des relations très étroites avec le gouvernement. Ces dernières aident principalement le gouvernement à promouvoir la normalisation à tous les niveaux et effectuent un travail de publicité et de formation en matière de normalisation auprès des autorités locales. Comme indiqué précédemment, les instances gouvernementales chinoises sont composées de multiples organes décisionnels. Chaque département (ministère ou bureau d'administration) relevant du Conseil d'État a ses bureaux au niveau des provinces et des municipalités, des districts, et des centaines de comtés. Ainsi, la coordination de l'ensemble de ces instances décisionnaires est un problème de longue date pour la normalisation chinoise. Si toutes ces organisations sont organisées selon un plan très hiérarchisé, en réalité, dans les faits, les normes locales, ministérielles ou sectorielles ont tendance à être plus appliquées que les standards nationaux, de par la prédominance des administrations locales et régionales dans les processus décisionnels en termes de mise en application des normes.

En 2015, le Conseil d'État de la RPC s'est engagé sur la voie d'une réforme visant à transformer fondamentalement le système de normalisation du pays d'ici 2020[219]. Afin d'accompagner la réforme de son système de normalisation, la Chine a fait appel à des experts américains, allemands,

[218] Standardization Administration of China (SAC)

français et britanniques, soulignant une nouvelle fois l'avance des pays occidentaux en matière de normalisation internationale. Ces efforts ont abouti à la création d'une nouvelle loi sur la normalisation adoptée en janvier 2018. Dans les faits, le nouveau système de normalisation chinois est aujourd'hui en quelque sorte hybride, à mi-chemin entre le contrôle et la surveillance de l'État, d'une part, et une ouverture vers les marchés privés, d'autre part. Tout d'abord, le gouvernement central a renforcé son pouvoir décisionnel en abolissant les normes industrielles et locales obligatoires, bien que des normes volontaires ou « recommandées » subsistent à ces niveaux[220]. Les deux catégories de normes obligatoires et recommandées subsistent au niveau national. Le but de ces réformes est de rationaliser et simplifier la production de normes par l'État central. Dans le même temps, l'espace pour les normes issues du marché s'est considérablement élargi. Outre les normes d'entreprise, héritées du système précédent, de nouvelles normes d'associations ont été introduites qui rassemblent des sociétés privées autour de la préparation d'une norme, une caractéristique qui ressemble davantage au système américain. Ce changement a notamment été opéré dans le but de galvaniser les efforts de collaboration au sein du secteur privé afin de favoriser l'innovation, ce qui reflète la reconnaissance croissante en Chine du rôle important que jouent les forces du marché dans le processus normatif. La participation des entreprises étrangères aux processus de normalisation a également été quelque peu simplifiée, et la plupart des Comités techniques sont ouverts à la participation de ces entreprises. Une série de lignes directrices publiées par la SAC, la Commission nationale du développement et de la réforme (CNDR) et le ministère du Commerce[221] stipule que les entreprises à capitaux étrangers ont droit au même traitement que les entreprises nationales lorsqu'il s'agit de participer à des travaux de normalisation. Ce principe a ensuite été codifié dans la loi sur les investissements étrangers de 2019[222], qui a introduit l'obligation pour l'État de garantir que les entreprises à capitaux étrangers puissent participer de manière égale à l'élaboration des normes (cf. figure 7).

---

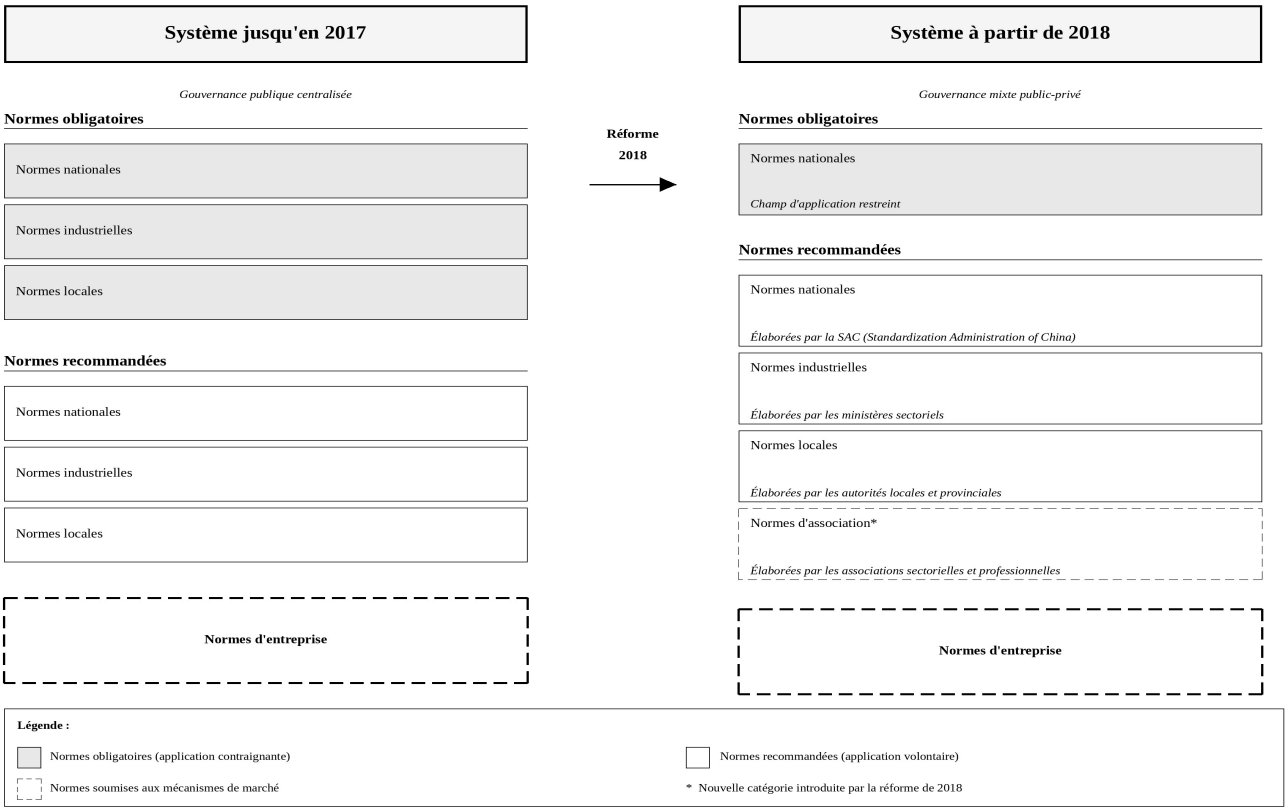
219 Conseil d'État de la République populaire de Chine, « Approfondissement du plan de réforme du travail de normalisation » (深化标准化工作改革方案), 11 mars 2015. Disponible ici : www.gov.cn

220 John Seaman, « China and the New Geopolitics of Technical Standardization », Ifri, janvier 2020.

221 Congrès national populaire, « Loi de normalisation de la République populaire de Chine », Beijing, 2017. Traduction anglaise disponible à l'adresse suivante : https://www.cfstc.org/en/2932583/2968817/index.html

222 Congrès national populaire, « Loi sur les investissements étrangers de la République populaire de Chine », Chine, 2019. Traduction anglaise disponible à l'adresse suivante : https://en.ndrc.gov.cn/policies/202105/t20210527_1281403.html

Figure 7 : Évolution du système de normalisation chinois : comparaison des structures jusqu'en 2017 et après 2018



Source : *Élaboration de l'auteur d'après John Seaman, « China and the New Geopolitics of Technical Standardization », Ifri, janvier 2020.*

Cependant, le système chinois de normalisation reste assez « byzantin », en conservant ses deux piliers que sont le contrôle de l'État et l'initiative privée, qui semblent pourtant en contradiction. D'une manière générale, l'approche de la Chine en matière de normalisation reste alignée sur la stratégie plus large de du pays en matière économique, qui vise à faire progresser l'intégration de la Chine dans le système économique mondiale. Au cœur de cette stratégie se trouve le principe « deux marchés, deux ressources », qui met en évidence deux objectifs liés : la protection du marché intérieur et l'intégration dans le marché international. Cette situation reflète la tentative du gouvernement chinois de réaliser la « quadrature du cercle » en introduisant des réformes économiquement libérales tout en gardant un fort

contrôle politique de l'État. Ce dernier impératif semble d'ailleurs s'être renforcé avec l'arrivée au pouvoir de Xi Jinping en 2012, qui a coïncidé avec un net renforcement de la surveillance du Parti communiste chinois (PCC) envers les sociétés privées, notamment étrangères[223]. Il reste à voir si les objectifs mis en avant par la réforme peuvent être atteints, mais, jusqu'à présent, l'une des conséquences a été une explosion du nombre de demandes de normes d'association, en partie due au fait que des incitations financières sont fournies simplement pour le dépôt d'une demande, que cette demande aboutisse à une norme ou non. La conséquence première de cela est que la forte implication de la Chine dans les processus de normalisation internationaux s'est souvent accompagnée d'une avalanche de nouvelles propositions de normes, pour la plupart rejetées[224]. La Chine a donc rapidement acquis la réputation de préférer la quantité à la qualité, poussant certains experts internationaux à s'interroger sur le bien-fondé de la nouvelle stratégie chinoise sur le long terme. En effet, si la Chine ne parvient pas à inverser la tendance et à se positionner comme un acteur doté d'une véritable force de proposition, cela risque d'endommager la réputation des experts chinois en normalisation sur le long terme. Cependant, les réformes du gouvernement chinois en matière de normalisation ne se sont pas arrêtées là.

Annoncée en mars 2018, la nouvelle stratégie chinoise de normalisation intitulée « China Standards 2035 » a provoqué un véritable « raz-de-marée » sur la scène internationale à la suite de sa publication. De nombreux observateurs y ont perçu une volonté agressive de la Chine de s'imposer dans le monde de la normalisation internationale, en particulier en Occident. Créé par la SAC et de l'Académie chinoise d'ingénierie (CAE), China Standards 2035 définit une nouvelle stratégie nationale de normalisation. Celle-ci est centrée en particulier sur les nouvelles technologies, avec comme objectif avoué de faire de la Chine le leader mondial dans la conception des nouvelles technologies, en devenant le leader du développement des normes dans ce domaine. En ce sens, China Standards 2035 est le direct héritier de Made in China 2025, publié en 2015, qui présentait la stratégie chinoise pour faire de la Chine l'acteur majeur de la production de biens à l'échelle mondiale. Comme le décrit la SAC elle-même : *« Les compagnies de première catégorie normalisent, les compagnies de second rang conçoivent les technologies, les compagnies de troisième ordre construisent les produits »*[225] . L'objectif affiché est donc clair, la Chine cherche à se positionner comme un leader mondial de la normalisation, domaine dans laquelle elle a pris un retard notable, afin de dominer la conception des nouvelles

---

223 Dana Heide, Tanja Kewes, Anja Müller, « Anti-Spionage-Gesetz beunruhigt deutsche Unternehmen », Handelsblatt, 20 juin 2023. https://www.handelsblatt.com/politik/deutschland/china-anti-spionage-gesetz-beunruhigt-deutsche-unternehmen/29211626.html

224 Propos recueilli auprès d'experts en normalisation durant la 56e réunion plénière de l'ISO/TC 211, Jeonju, Corée du Sud, 15 – 19 mai 2023.

225 Dieter Ernst, « Indigenous Innovation and Globalization: The Challenge for China's Standardization Strategy », UC Institute on Global Conflict and Cooperation and the East-West Center, juin 2011.

technologies émergentes qui seront le fondement de nos modes de vie futurs, en particulier dans le domaine des technologies de l'information et de la communication. Une grande attention sera accordée aux secteurs à forte valeur ajoutée, ou « développement de haute qualité », en particulier dans les domaines où les normes techniques n'ont pas encore été établies. Des domaines comme l'intelligence artificielle, le cloud, l'Internet des objets, la cybersécurité ou encore les données géographiques sont directement cités comme étant des domaines prioritaires pour la normalisation chinoise. De manière plus inquiétante, la stratégie chinoise se concentrera également sur les normes destinées à faciliter la fusion entre domaine civil et militaire, ce qui inquiète de nombreux acteurs, notamment américains. Ainsi, en 2021, le FBI a publié une note destinée aux représentants du secteur privé, mettant en garde contre les risques d'une mainmise chinoise sur la normalisation dans le domaine des hautes technologies, et sur le risque que cela représenterait pour la compétitivité des sociétés américaines[226] . Une réalité qui pousse certaines nations occidentales à faire participer leurs experts militaires aux réunions internationales de normalisation, notamment dans le domaine des normes géospatiales, où l'idée commence à circuler de plus en plus parmi les nations membres de l'OTAN[227]. Face à cette montée en puissance de la Chine dans des domaines technologiques de pointe, certains experts sont allés jusqu'à suggérer la création d'alliances en matière de normalisation rassemblant des nations démocratiques aux intérêts communs[228] une proposition pour l'instant restée lettre morte dans les milieux de la normalisation. De plus, en octobre 2021, la Chine a créé le « Programme national de développement de la normalisation[229] » annonçant la mise en place d'un mécanisme gouvernemental destiné à orienter les travaux de normalisation internationaux et à promouvoir les normes chinoises. Le programme comprendra la création de centres de recherche, d'innovation et de certification en matière de normes afin d'accélérer la capacité du pays à élaborer et à exporter des normes techniques. Bien que ce document souligne la participation accrue de l'industrie aux travaux de normalisation, reconnaissant ainsi l'importance du secteur privé en matière d'innovation concernant la création de norme, il renforce également le rôle dominant joué par le PCC et ses priorités politiques dans les stratégies de normalisation.

Couplé au projet des Nouvelles Routes de la Soie mis en avant depuis l'arrivée au pouvoir de Xi Jinping, la quête chinoise de domination des normes internationales fait également craindre une diffusion internationale, par le biais de programmes d'investissement de normes chinoises ou dirigées

---

226 Fédéral Bureau of investigation, « China's Standards 2035 Plan Seeks to Dominate Standards for Emerging, Disruptive Technologies, and ICT Global Marketplace », Liaison Information Report (LIR), LIR 210303004, 3 mars 2021.

227 Propos recueilli auprès d'experts en normalisation durant la dernière réunion plénière du DGIWG, Garmisch-Partenkirchen, 23-27 octobre 2023.

228 Jared Cohen et Richard Fontaine, « Uniting the techno-democracies: How to Build Digital Cooperation », *Foreign Affairs*, 13 octobre 2020. https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies

229 Central Committee of the Communist Party of China and the State Council, « Outline for the development of national standardization », Xinhua, 10 octobre 2021.

par des acteurs chinois, vers des pays ne disposant pas de l'expertise nécessaire pour choisir en toute connaissance de cause quelles normes adopter, laissant ainsi la Chine leur dicter lesquels choisir. Des choix pouvant mener certains pays à dépendre entièrement de produits normalisés par la Chine en matière d'infrastructure notamment. Ainsi, dans le cadre du développement des Nouvelles Routes de la Soie, la Chine a signé 85 accords de coopération en matière de normalisation avec près de 40 pays différents[230] . De fait, la mise en place d'un cadre architectural pour promouvoir la coopération en matière de normes et les moyens financiers massifs que la Chine déploie dans ce domaine font de Nouvelles Routes de la Soie et son projet-frère les Nouvelles Routes Numérique de la Soie constitue une formidable plateforme de diffusion des normes dans tous les domaines techniques[231] . La Chine s'est aussi lancée depuis de nombreuses années dans une politique de coopération économique fondée sur le partage de normes avec de nombreux pays en développement, par exemple avec *« le Mexique, qui a signé un protocole d'accord sur la normalisation en 2014, ou avec le Viêt Nam, le Laos, le Myanmar et l'Indonésie* » [232]. Dans ce domaine la Chine est en bien meilleure position pour agir en tant qu'organisme de normalisation et exporter ses normes afin de dominer le marché. Un des atouts de la Chine dans ce domaine tient au prix plus abordable des normes chinoises par rapport aux normes occidentales ou à celles produites par l'ISO, ces dernières parviennent plus facilement à séduire ces pays émergents, et la qualité des normes chinoises, de par leur implication de plus en plus forte au sein des organes internationaux de normalisation va crescendo ces dernières années, séduisant toujours plus d'acteurs. De plus, au vu de la forte implication de l'État chinois dans la stratégie nationale de normalisation de la RPC, et ce, malgré le remaniement de leur écosystème de normalisation, de nombreux experts ont soulevé des craintes quant au rôle des experts chinois, soupçonner de pouvoir favoriser des technologies dans lesquelles des entreprises chinoises ont déjà largement investi au moment de produire de nouvelles normes. Ainsi, la RPC a adopté une double approche pour renforcer la présence de la Chine dans la conception des normes technologiques de jure et de facto. En ce qui concerne la voie de jure, Beijing a cherché à influencer les organismes internationaux de normalisation (gouvernementaux) et les consortiums techniques mixtes. Cette approche consiste notamment à placer des ressortissants chinois à des postes de direction au sein de ces organismes, à accroître la représentation des entreprises technologiques chinoises, à occuper des postes de direction au sein des secrétariats, des groupes de travail et des sous-comités techniques, et à inciter les entreprises chinoises à voter en faveur des propositions chinoises. En dehors des organismes de normalisation, les entreprises

---

230 Daniel R. Russel et Blake H. Berger, « Stacking the Deck: China's Influence in International Technology Standards Setting », The Asia Society Policy Institute, 2021.

231 OECD Business and Financial Outlook, « China's Belt and Road Initiative in the Global Trade, Investment and Finance Landscape », OECD, 2018.

232 John Seaman, « China and the New Geopolitics of Technical Standardization », Ifri, janvier 2020.

chinoises diffusent des normes de facto en s'appuyant sur le projet des Nouvelles Routes de la Soie, avec l'aide de l'État chinois. En exportant ses technologies, en signant des protocoles d'accord pour l'harmonisation des normes et en développant d'autres mécanismes d'harmonisation des normes, Beijing propage ses propres normes technologiques dans les pays qui accueillent ces projets.

Certains craignent également que la Chine n'essaie de remodeler l'environnement actuel des normes internationales pour en faire un environnement davantage piloté par les États plutôt que les acteurs du marché. Certaines propositions avancées par des acteurs chinois au sein des organismes de normalisation, telles que la proposition « New IP » (visant à concevoir un nouveau système de protocole pour l'Internet) et une proposition relative à la normalisation de l'application de la reconnaissance faciale dans les systèmes de surveillance visuelle, ont suscité des inquiétudes quant à la possibilité que des acteurs chinois tentent d'utiliser la normalisation à mauvais escient pour promouvoir des technologies qui remettent en cause les valeurs démocratiques et les droits de l'homme. Ainsi, il apparaît que la promotion des normes chinoises dans la technologie mondiale est une conséquence de la stratégie du PCC visant à maximiser son influence sur la future économie mondiale. Cette stratégie est l'un des aspects d'un effort global visant à renforcer le pouvoir réglementaire du pays à l'échelle mondiale et à le protéger contre les contraintes ou les intrusions indésirables. Du point de vue de Beijing, le moment est venu de faire progresser les normes, les règles, les lois et les standards qui promeuvent et protègent les intérêts et la sécurité de la Chine. Cette détermination à consolider la place de la Chine dans l'ordre international et à le réformer est évidente, notamment dans les efforts de Beijing et du pays pour défendre sa conception de la cybersouveraineté à l'ONU, ainsi que dans la promotion et la diffusion de normes nationales par l'intermédiaire des organisations internationales de normalisation et du projet des Nouvelles Routes de la Soie[233]. Le fort soutien du gouvernement central envers certaines sociétés considérées comme capitales dans l'exploitation des nouvelles technologies, telles que l'IA[234], la 5G[235] ou le cloud, comme Huawei, soulève également des inquiétudes quant à la pénétration de ces sociétés au sein de consortiums privés de normalisation où l'implication financière est directement corrélée à la capacité de décision des acteurs impliqués. Ainsi, dans le domaine de la 5G, Huawei est aujourd'hui un géant de la normalisation avec 239 contributions en 2017, contre 214 pour Ericsson. Il y a maintenant plus de normes en Chine que dans n'importe quel autre pays (environ

---

233 Michael Sutherland, « CSR 2019 : Setting a New Standard: Implications of China's Emerging Standardization Strategy », SAIT China Studies Review, 29 octobre 2019.

234 Matt Sheehan, « China's New AI Governance Initiatives Shouldn't Be Ignored », Carnegie Endowment for International Peace, 4 janvier 2022. https://carnegieendowment.org/2022/01/04/china-s-newai-governance-initiatives-shouldn-t-be-ignored-pub-86127.

235 Paul Triolo et Kévin Allison. « The Geopolitics of 5G », Eurasiagroup, 15 novembre 2018. https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g

150 000), soit sept fois plus que dans l'Union européenne[236] . L'implication de certaines sociétés dans divers groupes de normalisation déjà établies, couplée à un fort soutien financier du Parti communiste chinois, pourrait conduire à un véritable monopole de ces entreprises sur certaines technologies.

Les informations géographiques sont citées dans le programme national de développement de la normalisation, comme faisant partie des technologies d'importance pour l'avenir. L'implication de la Chine au sein de l'ISO a grandement augmenté depuis ces dernières années, pour atteindre la sixième position en nombre de secrétariats pour l'ensemble des groupes de travail de l'ISO, soit un contrôle sur 10 % du total des groupes de travail. Cette tendance a également affecté l'ISO/TC 211 sur les informations géographiques et la géomatique. Ainsi, en 2023, sur les 128 projets de normes en préparation au sein du TC/211, 10 ont pour chef de projet un expert chinois. Un chef de projet est nécessaire pour le lancement de tout nouveau projet de norme, il est directement responsable du contenu du document normatif rédigé, et à pour responsabilité de s'assurer que le document respecte les règles définies par l'ISO/TC 211, non seulement sur la forme, mais également concernant les objectifs de la norme et doit s'assurer que ces derniers sont bien en adéquation avec les objectifs du comité technique. Les chefs de projet occupent donc un rôle capital pour la création d'un projet de norme, et pour la poursuite de ce projet tout au long de son cycle de développement. Enfin, 31 normes supplémentaires ont pour animateur des représentants chinois, soit plus de 1/3 des projets de normes au sein du T/211 ayant pour coordinateur technique ou politique un représentant chinois. L'animateur est un expert technique qui dirige l'élaboration des normes ISO au sein de son groupe de travail avec le soutien des chefs de projet et des experts internationaux qui y participent. L'animateur suit et assure l'avancement des travaux de normalisation ISO confiés à son groupe, et doit s'assurer de l'obtention d'un consensus. Là où le chef de projet doit avant tout assurer le pilotage du projet de norme et s'assurer de la bonne rédaction du document normatif, l'animateur assurer un rôle beaucoup plus proactif dans la gestion du groupe de travail dont il a la charge. Il doit ainsi s'assurer non seulement du bon déroulement des réunions de travail, il doit également activement rechercher d'éventuelles nouvelles exigences et évolutions techniques relatives à la norme développée. L'effort requis pour remplir le rôle d'animateur n'est pas négligeable. Les groupes de travail de l'ISO/TC 211 se réunissent chaque fois que nécessaire et au moins deux fois par an à l'occasion de la réunion plénière de l'ISO/TC 211, où l'animateur fait son rapport au comité technique. Le nombre d'animateurs et de chefs de projets au sein d'un comité technique et de ses sous-comités est donc un bon indicateur de l'implication d'un pays au sein d'un domaine de normalisation. Cela nécessite un important investissement humain et financier pour pouvoir coordonner les travaux de normalisation au sein d'un comité technique. Si

[236] N. Purnell et S. Woo, « China's Huawei is determined to lead the way on 5G despite US concerns », Wall Street Journal, 30 mars 2018.

l'augmentation de l'investissement chinois dans la normalisation des données géographiques semble donc avérée, il est intéressant de se pencher plus précisément sur les projets de normes auxquels la Chine participe. Ainsi, parmi les normes dont le chef de projet est un expert de la RPC, on retrouve les normes ISO/TS 19159-3 : 2018 – Calibration et validation de capteurs de télédétection – Partie 3: SAR/InSAR ; ISO/TS 19130-2 : 2014 – Modèles de capteurs d'images de géopositionnement – Partie 2: SAR, InSAR, lidar et sonar ; ISO/AWI TS 19124-2 – Calibration et validation des données de télédétection et des produits dérivés – Part 2: SAR ; ainsi que la norme ISO/TS 19159-4 : 2022 – Calibration et validation de capteurs de télédétection — Partie 4: Radiomètres spatiaux à micro-onde passive. L'intérêt chinois pour les normes en matière de calibration de capteurs de télédétections multispectraux n'est pas un hasard. Ainsi, en mars 2023, la Chine a lancé une nouvelle constellation de 36 satellites, dont 12 sont dotés de capteurs interférométriques radars (SAR), des produits de hautes technologies difficiles à produire et qui étaient jusqu'alors quasi absentes du parc de satellites chinois[237] . L'implication de la Chine dans la normalisation de tels capteurs est un indicateur dans son ambition dans le domaine spatial, et pourrait également indiquer une volonté de devenir exportateur de telles technologies, une fois l'ensemble des normes nécessaires à leur réalisation maîtrisé par les industries chinoises. Un autre domaine dans lequel la Chine s'est extensivement impliquée est celui des normes concernant le modèle d'administration des terres (Land Administration Domain Model [LADM]). Cette norme est divisée en six parties, dont chacune a pour animateur un expert chinois. La troisième partie de cette norme porte sur la régulation des espaces marins[238] . En mer de Chine du Sud, la RPC, en violation flagrante du droit international, proclame depuis de nombreuses années sa souveraineté sur l'ensemble de cet espace marin, empiétant du même coup sur les prétentions territoriales de nombreux pays en Asie du Sud-Est, comme les Philippines et le Viêt Nam. Un des leviers de l'ambition chinoise en mer de Chine tient au flou juridique qui entoure certaines règles de navigation au niveau du droit international, ainsi que certaines règles entourant la délimitation de la souveraineté sur les espaces marins[239] . Le soudain intérêt de la Chine pour une norme couvrant la géorégulation des espaces marins, qui vise en substance à codifier la réglementation entourant leur délimitation et l'affirmation du contrôle des États sur ces derniers, soulève des inquiétudes quant à la capacité de la Chine a faire plier les règles en sa faveur dans ce domaine afin de renforcer la légitimité de ses revendications en mer de Chine.

---

237 Andrew Jones, « China's SAR satellite surge continues with new constellation plan », Space News, 7 décembre 2021. https://spacenews.com/chinas-sar-satellite-surge-continues-with-new-constellation-plan/

238 ISO 19152-3 : Modèle du domaine de l'administration des terres (LADM) — Partie 3 : Géoréglementation marine.

239 Oriana Skylar Mastro, « How China is Bending the Rules in the South China Sea », Freeman Spogli Institute for International Studies, Stanford, 17 février 2021. https://fsi.stanford.edu/news/how-china-bending-rules-south-china-sea

3.3 Quelles conséquences concrètes pour l'écosystème normatif international ?

Même si « China Standards 2035 » semble décrire la stratégie chinoise en matière de normalisation comme étant une offensive à grande échelle visant à l'hégémonie chinoise sur les instances internationales de normalisation, il serait malvenu de prendre les déclarations grandiloquentes du Parti communiste chinoises pour argent comptant. Il faut garder à l'esprit que les plans quinquennaux et les grandes déclarations stratégiques, qu'il s'agisse de China Standards 2035 ou des nouvelles étapes du projet des Nouvelles Routes de la Soie, sont autant de déclarations d'intention dirigée vers les acteurs internationaux, mais également, si ce n'est avant tout, vers la population chinoise elle-même, afin de construire un discours positif sur le développement de l'économie chinoise et ses nouvelles opportunités de développement. Il est donc nécessaire de garder un certain recul face à ces déclarations et d'observer si oui ou non, la Chine a les moyens de ses ambitions, et si ces dernières sont nécessairement synonymes de mauvaises nouvelles pour le reste de la communauté internationale.

Tout d'abord, il est nécessaire de garder à l'esprit que la participation croissante de la Chine à la normalisation internationale est une bonne nouvelle pour l'écosystème normatif mondial. Cela signifie qu'elle intègre des acteurs mondiaux qui considèrent les instances internationales de normalisation comme utiles. Cela indique également que les acteurs chinois préfèrent s'engager dans des organisations qui soutiennent l'ordre international plutôt que d'essayer de le subvertir, et que la Chine, dans l'ensemble, souhaite faire partie du système mondial de normes (et, implicitement, du commerce), plutôt que de s'en dissocier. Une participation accrue à la normalisation a, en général, des implications positives. Elle permet une plus grande diversité de pensées et de points de vue, crée davantage d'occasions de renforcer et d'améliorer les propositions de normes, et signifie que les normes adoptées sont fondées sur un consensus international plus large, ce qui augmente potentiellement les chances qu'elles soient déployées sur le marché à une plus grande échelle[240] . La participation de la Chine pourrait avoir des conséquences positives sur l'interopérabilité mondiale et la sécurité des produits et des services. Elle pourrait également renforcer l'acceptation et l'adoption des normes internationales au niveau national, réduisant ainsi les obstacles au marché pour les entreprises étrangères. Ces aspects sont particulièrement importants, étant donné que la Chine est un grand exportateur de biens et un grand marché pour les biens importés. De plus, le fait que les acteurs chinois soient davantage exposés et familiarisés avec le fonctionnement de la normalisation internationale et les principes et procédures qui

[240] Sorina Teleanu, « The geopolitics of digital standards: China's role in standard-setting organisations », DiploFoundation & Multilateral Dialogue Konrad Adenauer Foundation Geneva, 2021.

y sont appliqués (par exemple, la transparence et le consensus) pourrait se traduire par des améliorations dans le système chinois de normalisation.

Ainsi, ce serait une grave erreur de réagir de façon trop antagoniste à la montée en puissance de la Chine au sein de l'écosystème normatif international. En tant que deuxième puissance économique mondiale, et rassemblant une si large part de sa population, la montée en puissance de la Chine est loin d'être une anomalie, et correspond plus au contraire à un rééquilibrage du paysage normatif international, plus proche des réalités mondiales en termes de conception et de consommation de produits. Exclure ou isoler la Chine dans la normalisation internationale ne serait bénéfique pour personne sur le long terme. En particulier pour la France, et l'ensemble des pays de l'Union européenne qui seraient mis en difficulté très rapidement en cas de polarisation du milieu normatif mondial. Si la Chine devait de nouveau se retirer des espaces de normalisation internationaux, au nom d'un sentiment de rejet de la part des Occidentaux depuis toujours en position dominante au sein des instances internationales de normalisation, cela pourrait pousser la Chine à construire auprès d'autres États en développement proches de leurs intérêts, un véritable espace normatif parallèle aux organismes de normalisations internationaux actuels. Une telle situation entraînerait une véritable « Guerre froide » normative qui diviserait le marché mondial le long de lignes idéologiques. Ce serait alors un véritable désastre pour les économies de l'espace européen, qui se verrait fermer l'accès non seulement au très important marché chinois, mais également à celui de tous les pays ayant préféré rejoindre l'espace chinois de normalisation, par choix ou contrainte économique. Cela obligerait les sociétés qui voulaient pénétrer ces marchés à développer des lignes de production spécifiques respectant les nouvelles normes de ce nouvel espace économique, entraînant des coûts faramineux pour ces sociétés, et en fermant de facto l'accès à ces marchés à grand nombre d'entre elles. De plus, une telle situation rendrait les économies européennes bloquées dans un espace « occidental » de plus en plus vulnérable à la pression américaine dans ce domaine, de par son poids économique très important au sein d'un tel espace, qui ne manquerait pas de renforcer son investissement au sein des organisations de normalisation internationales au sein de cet espace, avec à sa disposition une capacité d'investissement et de mobilisation en termes de personnel inégalé en comparaison des autres acteurs.

Si l'exclusion de la Chine des organisations internationales de normalisation ne peut en aucun cas être considérée comme une option viable, quelle stratégie un pays comme la France peut-il adopter pour continuer à protéger ses intérêts ? Tout d'abord il faut prendre conscience qu'il serait plus efficace que les discussions se concentrent moins sur la Chine et sur les moyens possibles de répondre à son implication, et davantage sur ce qui peut être fait pour maintenir l'intégrité globale de l'écosystème normatif international. Il convient de veiller à ce que les processus de normalisation internationaux continuent à fonctionner selon des règles bien établies, à ce que des cadres de surveillance et de

responsabilité pertinents soient en place et à ce qu'aucun acteur, quel qu'il soit, ne soit en mesure de manipuler le système. Un des premiers piliers pour protéger cette intégrité est de continuellement chercher à étendre le champ des acteurs participants aux processus de normalisation. Dans le domaine de la normalisation des informations géographiques, cela reviendrait par exemple, à chercher à étendre le champ des pays membres du TC/211, qui est loin de compter l'ensemble du globe à l'heure actuelle. Plus les acteurs sont nombreux, moins le risque de voir des décisions monopolisées par un petit nombre d'acteurs ne grandit. Un autre point sur lequel il est nécessaire de se pencher tient aux ressources allouées à la normalisation par les différents acteurs. Comme nous l'avons vu précédemment, la normalisation est loin de se résumer à un processus objectif entre experts pour la sélection des meilleures technologies disponibles. Pour peser dans le monde de la normalisation internationale, les pays doivent pouvoir disposer d'experts compétents, en nombre suffisant, et leur offrir les moyens de participer efficacement aux processus de décisions et aux délibérations qui précèdent l'adoption d'une norme. Cela demande un investissement économique et humain important, qui est souvent sous-estimé pour qui n'est pas directement au fait du fonctionnement des instituts de normalisations, qu'ils s'agissent de l'ISO ou de consortiums privés. Ainsi, selon les calculs d'une experte américaine du secteur des hautes technologies, *« il en coûte en moyenne 300 000 dollars par an aux entreprises pour financer les services d'un seul ingénieur qui travaille à plein temps sur les normes techniques et participe aux réunions internationales »*[241].

La meilleure façon pour des pays comme la France de maintenir leur place en tant qu'acteur majeur de la normalisation internationale est de se concentrer sur leur propre participation et de donner à leurs experts les moyens de leurs ambitions en renforçant non seulement leur nombre, mais aussi en étant capable de les fidéliser afin de pouvoir bénéficier de leurs capacités de négociations sur le long terme. La normalisation est le domaine du consensus, et le capital humain accumulé par les experts en normalisation travaillant depuis de nombreuses années dans leur domaine de spécialité compte autant, si ce n'est plus encore que leurs compétences techniques. La définition d'une stratégie nationale en matière de normalisation, telle que la France le fait depuis plusieurs années, est un bon moyen de maintenir des objectifs précis à l'échelle nationale en matière d'investissement et de participation dans ce domaine. Idéalement il faudrait décliner cette stratégie pour chaque domaine technique. Continuer à inciter un maximum d'acteurs privés à devenir membres de consortiums privés de normalisation afin de renforcer la présence industrielle du pays au sein de ces organes de décision doit également être une nécessité de tous les instants pour réaliser les objectifs de la stratégie nationale de normalisation.

---

[241] Whalen Jeanne, « Government Should Take Bigger Role in Promoting U.S. Technology or Risk Losing Ground to China, Commission Says », *Washington Post*, 1er décembre 2020.

Un autre point important mis en avant par le modèle chinois est le développement de cursus universitaires dédié à la normalisation. Dans China Standards 2035, la Chine a annoncé comme objectif de multiplier les cursus de ce genre au sein de ses universités pour engendrer un maximum de spécialistes en normalisation dans tous les domaines techniques jugés critiques. En effet, la Chine compte depuis 2010 environ 200 parcours universitaires dédiés à la normalisation. Il s'agit probablement d'un des aspects les plus cruciaux à analyser lorsque l'on observe la stratégie chinoise de normalisation. Les diplômes en normalisation restent une exception dans le monde et très peu de pays en disposent. Ces derniers se sont progressivement développés, en particulier en Asie de l'Est. Ainsi, en 2005, la Corée du Sud a été le premier pays à officiellement lancer un programme universitaire dédié à la formation en normalisation, en 2011, le pays comptait 81 parcours universitaires dédiés à la normalisation répartie dans 41 universités. Entre 2003 et 2006, la Thaïlande a financé l'ouverture de programme d'enseignement secondaire sur la normalisation. Dans le même temps, le Japon leur a emboîté le pas en finançant entre 2005 et 2010 l'ouverture de 51 parcours universitaires dédiés à la normalisation[242] au sein de ses universités. L'Indonésie a également financé l'ouverture de formation en normalisation au sein de dix de ses universités dès 2007. En Europe, les établissements d'enseignement supérieur ne disposent que d'une infrastructure académique très limitée dans le domaine de la normalisation, il n'existe pas de programme d'études avec un contenu de base défini ni de manuel reconnu internationalement sur l'enseignement des rouages de la normalisation. On observe aujourd'hui que le nombre total d'étudiants en normalisation dans tous les pays européens s'élève probablement à 1 000[243]. En France très peu d'universités disposent des diplômes dédiés à former à la normalisation internationale. On peut tout de même citer l'université technologique de Compiègne, qui délivre un diplôme de Master en normalisation depuis 2007[244], ou encore l'École Internationale des Sciences du Traitement de l'Information (EISTI) qui a introduit un programme sur la normalisation au sein de son Master en intelligence économique depuis 2009[245]. Force est de constater que la montée en puissance de la Chine sur la scène internationale doit nous alerter sur la possible nécessité de développer plus de cursus universitaires de ce genre si la France veut pouvoir continuer à peser à l'avenir dans les forums internationaux de normalisation.

En conclusion, s'il apparaît évident au vu des évolutions récentes que la participation accrue de la Chine au sein de la normalisation internationale est le produit d'une stratégie de domination des

---

242 Hesser Wilfried, « Memorandum on Standardization in higher Education in Europe », Hambourg, Allemagne, 2014.

243 Henk J. de Vries et Tineke M. Egyedi, « Standardization Education : Developments and Progress », *New Applications in IT Standards: Developments and Progress*, janvier 2010.

244 ISO, « A French university: Encouraging hands-on experience », 2007. https://www.iso.org/sites/materials/initiatives-in-education/education_initiatives-higher-edu/educational_materials-detail-initiatives8111.html?emid=10

245 ISO, « France - Fostering competitive intelligence », 2009. https://www.iso.org/sites/materials/initiatives-in-education/education_initiatives-higher-edu/educational_materials-detail-initiatives6833.html?emid=124

normes, cette dernière a l'avantage d'être pleinement exposée au reste du monde. Si cela représente indéniablement un défi pour la gouvernance mondiale de la normalisation, et accroît les risques d'une politisation du processus normatif, au risque d'éroder l'efficacité de ce dernier, rien ne permet d'affirmer aujourd'hui que la Chine a corrompu les institutions internationales de normalisation. S'il est naturel pour les nations occidentales de garder un œil sur une puissance économique concurrente aussi importante que celle de la Chine, il faut garder à l'esprit que les outils dont usent les experts chinois (à savoir leur participation et leur investissement humain et financier) pour parvenir à faire adopter leurs idées sont les mêmes que ceux à dispositions des autres pays. En d'autres termes, s'il était naïf d'observer sans réagir cette résurgence chinoise dans le monde de la normalisation, seule une participation accrue permettra aux pays qui s'en méfient de continuer à tirer leur épingle du jeu. Pour cela, il est important que la France et ses alliées continuent à investir suffisamment de temps et d'argent à la fois pour garantir la présence de leurs experts au moment des délibérations, mais également afin de pouvoir apporter des solutions toujours plus innovantes et respectueuses des valeurs défendues par ces derniers, qui sont les conditions sine qua non du maintien de la compétitivité occidentale dans le domaine de la normalisation. Plutôt que de chercher à contrer une influence chinoise réelle ou perçue, il serait plus judicieux de se concentrer sur l'amélioration des propositions futures en matière de normes, tout en s'appuyant sur le vaste réseau de relation de confiance nouée par nos experts en normalisation auprès des autres experts internationaux, dont les intérêts sont alignés avec les nôtres, qui ont un rôle crucial dans le soutien apporté à nos propositions de normes et celles de nos alliés.

Conclusion du Chapitre I

Ainsi, la normalisation est donc un enjeu de premier plan pour tous les États industrialisés, et ce, depuis son institutionnalisation au début du XXe siècle. L'attention accordée à la normalisation n'a fait que grandir après la Seconde Guerre mondiale et la création de l'ISO qui formaliser le champ de la compétition et de la coopération en matière de norme à l'échelle internationale, faisant de la normalisation, un élément indispensable pour toute société cherchant à pénétrer le marché mondial dans une économie mondialisée, et ce, quel que soit le domaine technique visé par l'entreprise. L'avènement de la normalisation internationale et la victoire du libéralisme à l'échelle mondiale a également fait éclater au grand jour les enjeux géopolitiques de la normalisation. Autrefois majoritairement un outil au service du protectionnisme économique destiné à protéger les économies nationales en empêchant la pénétration de leur marché par des sociétés étrangères, les normes, en devenant international, sont devenues des outils de fluidification des échanges en permettant à des sociétés d'aligner leur production sur des critères reconnus internationalement et de pénétrer des marchés autrefois inaccessibles. Si les normes peuvent toujours constituer des entraves aux échanges, l'internationalisation des normes les a également ouvertes à la compétition internationale entre sociétés et entre États, voire entre les États et sociétés privées, dans le but de maîtriser les normes, et avec elles, le marché. Portant en elles des enjeux politiques, économiques et éthiques, les normes participent à façonner les technologies de demain, et avec elles notre future. Les normes en matière de données géographiques numériques n'échappent pas à ces dynamiques à l'heure où ces dernières sont produites à une échelle encore jamais vue auparavant par un nombre d'acteurs privés et publics grandissant. Le champ d'application très large de ces données et l'importance de leur maîtrise pour les gouvernements, tant pour la gestion de leur territoire que sa protection, fait de la maîtrise des normes en matière d'information géographique un enjeu de premier plan pour les États modernes. Aujourd'hui l'échelle internationale constitue l'échelle privilégiée de la normalisation en matière d'informations géographiques. Cette dernière prend place au sein d'un véritable écosystème d'organisations et de parties prenantes diverses dont il faut analyser le fonctionnement pour comprendre comment ces acteurs interagissent et la place de la France au sein de ce dernier. C'est là-dessus que se concentre le chapitre suivant. Dans un premier temps nous verrons la place des principaux organismes de normalisation internationaux et des consortiums privés impliqués dans la normalisation des données géographiques numériques. Dans une seconde partie sera exposé le fonctionnement de la normalisation européenne et ses acteurs. Enfin la troisième partie de notre exposé sera dédié aux organes de la normalisation des données géographiques dédiés aux armées.

Chapitre II- L'écosystème de la normalisation des données géographiques

1. Les organismes internationaux et consortiums privés au cœur de la normalisation des données géographiques

Comme pour l'ensemble des domaines techniques concernés par la normalisation, l'écosystème normatif des données géographiques numériques est composé à la fois des instances internationales de normalisation que sont l'ISO et l'IHO et de consortiums privés formés par des industries du secteur, comme l'OGC. Il faut également prendre en compte les organismes de normalisation de l'Union européenne qui jouent un rôle capital non seulement pour la normalisation des acteurs européens, mais également d'autres acteurs internationaux, en fixant les règles en matière de normes pour l'ensemble du marché européen. Les institutions européennes de normalisation sont également représentées à l'ISO et portent parfois des projets communs au sein des instances internationales. L'ensemble de ces organisations forment l'écosystème international de la normalisation des données géographiques numériques, et rassemblent des acteurs différents et fonctionnent également de façon différente. Il est donc nécessaire de se pencher sur la façon dont ces différents organismes interagissent entre eux et façonne la normalisation de ces données, et les stratégies déployées par différentes parties prenantes au sein de ces derniers.

1.1. L'Organisation internationale de normalisation (ISO)

L'ISO est une organisation non gouvernementale, fondée en 1947. L'ISO est née de l'union de deux organisations, l'ISA (Fédération internationale des associations nationales de normalisation) et l'UNSCC (Comité de coordination de la normalisation des Nations unies). Après l'union de l'ISA et de l'UNSCC, l'ISO a été créée à l'issue de discussions tenues lors d'une conférence à Londres en octobre 1946, à laquelle ont participé 65 délégués de 25 organismes nationaux de normalisation. La mission de l'ISO est de « *promouvoir le développement de la normalisation et des activités connexes dans le monde en vue de faciliter les échanges internationaux de biens et de services et de développer la*

coopération dans les domaines de l'activité intellectuelle, scientifique, technologique et économique »[246].

La structure décentralisée de l'ISO est l'une de ses caractéristiques principales. Les travaux techniques se déroulent au sein des Comités techniques (CT), dont les secrétariats sont assurés par les membres de l'ISO et gérés et coordonnés par le Bureau de Gestion technique (BGT). Les réunions des CT et de leurs sous-comités (SC) ont lieu dans le monde entier. Les CT/SC sont des organes ouverts : chaque organisme membre (membre à part entière) intéressé par le sujet traité par un TC/SC établi peut devenir un membre actif (membre P) ou un observateur (membre O.), selon le degré d'implication qu'il souhaite avoir dans les travaux du comité. Les membres correspondants peuvent s'inscrire en tant qu'observateurs, mais sans droit de commentaire ni de vote.

Les CT sont créés et dissous par le Bureau de gestion technique (BGT). Chaque CT est responsable de l'élaboration de normes dans un domaine prédéfini (délimité par son champ d'application). Une proposition de nouveau domaine de travail peut émaner d'un organisme national, d'un CT/SC, d'un Comité chargés de l'élaboration d'orientations politiques (CCP), du BGT, du SG, d'un organisme de certification ou d'une autre organisation. Un nouveau TC ne peut être établi que si les deux tiers des membres votants de l'ISO (membres à part entière) y sont favorables et qu'au moins 5 d'entre eux s'engagent à y participer activement. Le BGT peut également décider de confier le travail à un CT existant ou de créer un comité de projet (CP) pour un projet unique ne relevant pas du champ d'application d'un CT existant. Un CP est généralement dissous une fois qu'il a publié sa norme. Les CT peuvent créer des sous-comités (SC) par une décision prise à la majorité des deux tiers des membres du CT, décision qui doit être ratifiée par le BGT.

Chaque TC/SC est présidée, pour une durée maximale de neuf ans (trois mandats de trois ans), par un expert dans le domaine. Les groupes de travail sont présidés par des *« animateurs »*[247] *»* et chaque projet est dirigé par un *« chef de projet »*[248] *»* Les *« Présidents »*[249] *» et* les *« Secrétariats »*[250] doivent agir à titre international, ce qui signifie qu'un Président ne peut pas être également le délégué d'un organisme national au sein de son propre comité. Les présidents, les chefs de projet, les secrétaires et les organisateurs doivent rester neutres, agir en tant que facilitateurs pour parvenir à un consensus entre les experts/membres de l'ISO et ne pas essayer d'influencer le travail du comité.

---

246 Directives de l'ISO/IEC, Introduction.
247 Directives de l'ISO/IEC Partie 1, Clause 1.12.
248 Directives de l'ISO/IEC Partie 1, Clause 2.1.8.
249 Directives de l'ISO/IEC Partie 1, Clause 2.8.2.
250 Directives de l'ISO/IEC Partie 1, Clause 1.9.2.

Le consensus est le principe clé qui sous-tend la prise de décision dans le système ISO et l'une des principales tâches des responsables des comités de l'ISO est d'être en mesure d'établir un consensus et de reconnaître qu'un consensus a été atteint. Dans de nombreux cas, notamment en ce qui concerne l'avancement des travaux techniques, les directives ISO/CEI définissent des critères spécifiques pour l'approbation des décisions (par exemple, vote à la majorité simple ou à la majorité des deux tiers). Les processus décisionnels varient également légèrement entre les différents organes de gouvernance, en fonction de leurs fonctions.

À l'exception des amendements aux statuts qui requièrent une « super majorité » des trois quarts des organes membres, les décisions de l'AG et des réunions du Conseil sont prises à la majorité simple des membres. Les décisions adoptées par correspondance sont prises à la majorité des deux tiers ou à la majorité relative dans le cas de propositions comportant de multiples alternatives. Cependant, au cours des réunions, la plupart des décisions sont prises sans vote formel, une fois qu'un consensus a été trouvé entre les membres réunis. En outre, au sein du Conseil et du Comité de gestion technique, les membres sont censés représenter les intérêts de la communauté ISO dans son ensemble, et *« ne pas prendre en considération leurs intérêts nationaux »*[251].

Dans les travaux techniques, le processus de prise de décision doit garantir une large adhésion au contenu de la norme, une norme internationale exigeant un « double niveau de consensus », d'abord parmi les experts (au sein du groupe de travail), puis parmi les organismes membres (au niveau du comité technique/de la commission technique et au stade de la publication). Dans le système ISO, le consensus est défini comme un *« accord général, caractérisé par l'absence d'opposition soutenue à des questions substantielles de la part d'une partie importante des intérêts concernés et par un processus qui implique de chercher à prendre en compte les points de vue de toutes les parties concernées et à réconcilier les arguments contradictoires »*[252].

Il incombe donc aux organisateurs (stade préparatoire) ou au président du CT/SC (stade comité) d'évaluer si un consensus a été atteint et de décider de passer à l'étape suivante, dans les cas où un vote formel n'est pas nécessaire. Deuxièmement, pour les étapes où un vote est requis, les critères d'approbation sont fixés de manière à refléter une large adhésion parmi les membres de l'ISO. Par exemple, une norme internationale n'est approuvée que si une majorité des deux tiers des membres P votants du CT/SC y est favorable et que pas plus d'un quart des membres de l'ISO votants n'émet un vote négatif.

Ainsi, une norme est approuvée par les membres qui participent activement à l'élaboration de cette norme et par ceux qui en ont besoin sur le marché, c'est-à-dire les membres P, mais elle peut

---

[251] Règlement intérieur du Conseil, Clause 2.7 ; Règlement intérieur des Comités de Gestion technique, Clause 3.

[252] ISO/IEC guide 2, *Normalisation et activités connexes — Vocabulaire général*, 2004.

néanmoins être bloquée par une minorité d'organismes membres de l'ISO (les membres à part entière). Ces deux paramètres combinés garantissent que la norme publiée est largement reconnue au niveau international. En outre, les comités membres ont recours à un mécanisme d'appel s'ils estiment que les règles et procédures de l'ISO n'ont pas été correctement appliquées ou si les actions ou inactions d'un comité pouvaient avoir de graves conséquences négatives, en particulier lorsqu'elles ne sont pas *« dans le meilleur intérêt du commerce international ou de facteurs publics, tels que la sécurité, la santé ou l'environnement »*[253]. De plus, dans le domaine technique, les votes négatifs doivent être justifiés pour être valables. Si aucune justification n'est fournie, le vote négatif n'est pas enregistré. Cette exigence facilite les tentatives de résolution des votes négatifs et la recherche d'un consensus. Les secrétaires doivent prendre en compte tous les commentaires et justifier le rejet d'un commentaire.

Tant dans le domaine politique que technique, les votes peuvent être effectués par correspondance, à l'aide d'un système de vote en ligne. Il est également parfois possible de participer à des réunions à distance. Cela facilite la participation de tous, en particulier des membres et des parties prenantes des pays en développement, qui ne peuvent pas toujours assumer les frais de déplacement. En ce qui concerne les organes de gouvernance de l'ISO, l'AG et le Conseil adoptent la plupart de leurs décisions lors de réunions, tandis que le TMB adopte environ 100 décisions par an par correspondance[254] . Dans les comités techniques, une grande majorité des décisions sont prises par correspondance. Avec une moyenne de 7 500 votes par an[255] le système de vote en ligne est une ressource clé pour faciliter la prise de décision à l'ISO et encourager la participation la plus large possible.

253 Directives de l'ISO/IEC Partie 1, Clause 5.1.2.

254 Justus Baron et coll., « Making the Rules: The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights », *TILEC Discussion Paper,* Tilburg University, octobre 2019.

255 *Ibid*.

1.1.1 L'ISO/TC 211 : Informations géographiques/géomatique

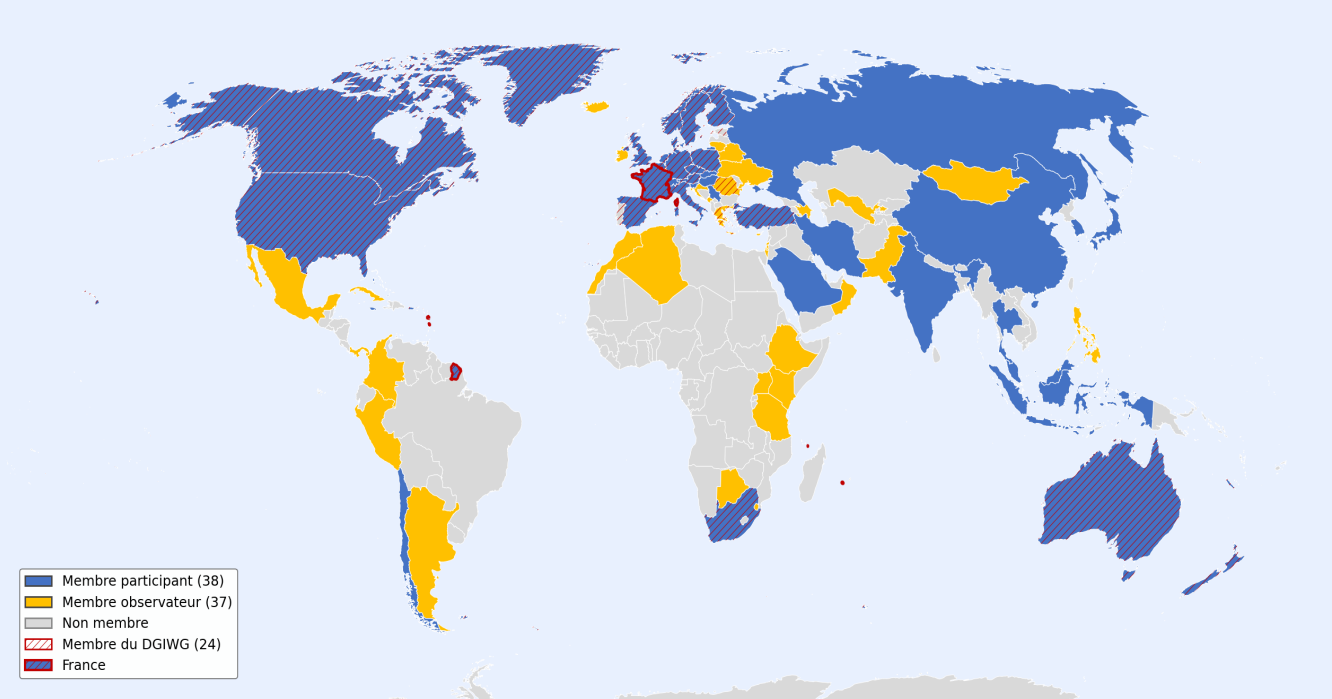
L'ISO/TC 211 a été fondé en 1994. Son prédécesseur est un comité de normalisation européen ayant un champ d'application comparable. Il s'agit du CEN/TC 287 « Information géographique ». Les titres des 20 normes de base de la famille ISO 19100 avaient déjà été définis par le Comité technique 287 du CEN. En 1994, les États-Unis et le Canada, avec le soutien de l'OTAN, ont proposé d'étendre la normalisation de l'information géographique à une plateforme mondiale. C'est ainsi qu'est né l'ISO/TC 211. Aujourd'hui, l'ISO/TC 211 est composé de 75 organismes étatiques, dont 38 membres participants (membres P), et 37 membres observateurs (membres O.)[256] (cf. carte 3). La majorité de ces membres se trouvent en Europe et en Amérique du Nord ou en Asie de l'Est. L'Amérique du Sud et le continent africain restent largement sous-représentés. Ainsi, en Amérique du Sud, seul le Chili est membre participant, tandis qu'en Afrique, seule l'Afrique du Sud l'est. Cette disparité s'explique en grande partie par un manque de moyens financiers et humains dans ces pays. Il faut également prendre un compte une certaine méconnaissance de l'intérêt de participer à des programmes de normalisations internationaux, qui persiste encore dans beaucoup de régions du monde. De plus, les données géographiques sont souvent perçues à tort comme un domaine de niche, ce qui ne pousse pas certains acteurs à s'y intéresser.

Il existe également 38 organismes externes de liaisons, qui font le lien entre l'ISO/TC 211 et d'autres organisations ayant un intérêt dans la normalisation des données géographiques. L'OGC est de loin la plus importante de ces organisations externes. 29 organisations internes existent aussi pour faire le lien entre certains comités techniques d'autres SDO, comme l'ISO/TC 20/SC 14 « Space systems and operations ». Seuls les organismes étatiques des membres participants disposent d'un droit de vote. Tous les autres n'ont que le droit de commenter. Un comité conjoint de l'ISO et de la Commission électrotechnique internationale (CEI), appelé Comité technique mixte ISO/CEI 1 (ISO/CEI JTC 1) sur les technologies de l'information, possède deux sous-groupes qui développent des normes d'un intérêt particulier pour la communauté des normes géographiques. Le sous-comité 24 de normalisation des technologies de l'information, Infographie et traitement de l'image (ISO/IEC JTC 1/SC 24) prépare des normes pour l'infographie et le traitement de l'image, largement fondées sur des consortiums privés ou des normes de facto avec une large utilisation commerciale/technique. Le sous-comité 29 de la normalisation des technologies de l'information, Codage du son, de l'image, de l'information multimédia et hypermédia (ISO/IEC JTC 1/SC 29), normalise le codage de l'information audio, image, multimédia et hypermédia, ainsi que des ensembles de fonctions de compression et de contrôle à utiliser avec l'information audio, l'image fixe et l'image animée.

[256] Site officiel de l'ISO/TC 211 https://committee.iso.org/sites/tc211/home/about/p--and-o-members.html

Les normes élaborées par l'ISO/TC 211 sont souvent appelées la famille ISO 19100, car leur numéro va d'ISO 19101 à ISO 19175 avec la possibilité d'une extension jusqu'à ISO 19199.

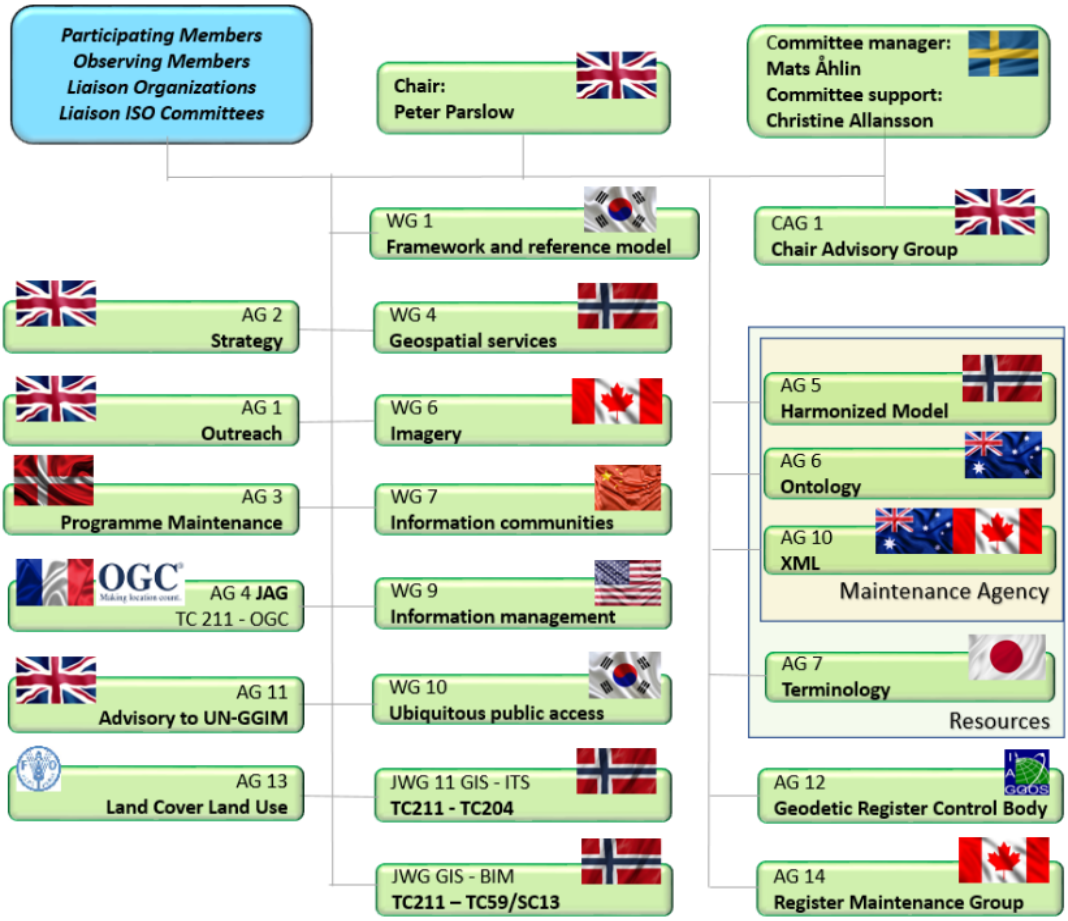
Carte 3 : Pays participants à la normalisation géospatiale mondiale (2024)



Source : *Site officiel de l'ISO/TC 211 et du DGIWG (2024)*

Les normes au sein de l'ISO/TC 211 sont rédigées par des groupes de travail (WG) et deux groupes de travail communs (Joint Working Group [JWG]), qui se concentrent chacun sur des groupes de normes spécifiques. Ces groupes de travail sont aidés par des groupes consultatifs qui conseillent les membres des groupes de travail sur certains aspects précis de leur travail. Les groupes de travail sont au nombre de huit et couvrent l'ensemble des domaines concernés par la normalisation des données géographiques, du maintien des cadres et modèles de références (WG1) qui fournissent le cadre procédural dans lequel les groupes de gestion des ressources travaillent et le cadre que les groupes de travail utilisent, en passant par les services géospatiaux (WG4), l'imagerie (WG6) ou encore les communautés d'information (WG7) qui se concentre sur les questions de normalisation liées à la modélisation conceptuelle des entités géographiques, y compris la documentation des entités géographiques dans les catalogues d'entités, les dictionnaires et les registres (cf. Figure 8).

Figure 8 : Répartition des différents groupes de travail de l'ISO/TC 211



Source : *Site officiel de l'ISO/TC 211 (2024)*

La gouvernance des différents groupes de travail et de conseil au sein de l'ISO/TC 211 est un bon reflet de l'implication des différents États au sein de ce comité technique. Au sein de l'ISO/TC 211, la France dirige le groupe de conseil joint AG4 JAG TC 211-OGC avec l'OGC, qui s'assure de la coordination entre l'OGC et l'ISO. Cette coopération est un pilier de l'interopérabilité des normes géospatiales en facilitant le développement de normes interopérables par les deux plus larges organisations de normalisation dans cette catégorie. Le poste de président est occupé par M. Sarafinof, qui a été réélu à sa tête en décembre 2022, assurant le maintien de la présidence française de ce comité au sein de l'ISO/TC 211. Si on retrouve encore une fois une majorité de pays occidentaux, notamment européens aux commandes de la plupart des groupes de travail et de conseil, comme la Norvège (4 groupes de travail), ainsi que l'Angleterre (4 groupes de travail et à la tête de la présidence de l'ISO/TC 211), la répartition des secrétariats de groupes de travail souligne une autre tendance au sein de l'ISO/TC 211.

En effet, la présence marquée de plusieurs pays est-asiatiques est notable. Si la présence du Japon est peu surprenante du fait de son investissement de longue date dans la normalisation internationale, celles de pays comme la Chine et la Corée du Sud sont à souligner. Cette dernière est à

la tête du WG1 sur les cadres et modèles de référence. Ce groupe de travail est un des plus fondamentaux de l'ISO/TC 211 en ce que ces normes sous-tendent toute l'architecture sur laquelle est fondé le développement des autres normes de l'ISO/TC 211. Parmi les projets de normes en cours au sein de ce groupe de travail se trouve l'ISO 19104 - SMART Terminologie pour l'information géographique. Cette nouvelle norme a vu son premier comité organisé en octobre 2022. Le but de cette norme est la création d'un registre unique des terminologies provenant des projets publiés et des projets en cours de développement. Une fois cette norme entrée en application, le registre unique de terminologie pourra être mis à jour en temps réel, et non plus uniquement une fois par an comme actuellement. Le travail mené prend appui sur des exemples de cas d'usage donné par l'OGC. La France suit attentivement ce projet, mais s'est abstenue lors de ce premier comité et met en garde contre le risque de privilégier une solution propriétaire au détriment d'une solution plus collaborative (fonte XML, SMART)[257]. Enfin, la Corée du Sud est également à la tête du WG10 « accès public universel ». Ce groupe de travail se concentre notamment sur le développement de normes ayant trait aux villes intelligentes et à leur interconnexion, un domaine en pleine expansion à sein de la communauté des informations géographiques. L'ISO 19171 — Traitement des objets urbains dans les villes intelligentes, ainsi que la norme ISO/TR 19174 — sécuriser l'interopérabilité entre des modèles d'information hétérogènes de villes, sont toutes les deux développés au sein du WG10. Ces projets sont d'un intérêt particulier pour la Corée du Sud, qui investit massivement dans le développement des villes et infrastructures intelligentes. Ainsi, lors de la 56e réunion plénière de l'ISO/TC 211 à Jeonju, les représentants sud-coréens ont présenté leur dernier modèle de ville intelligente, un modèle extrêmement avancé qui a fait forte impression lors de leur démonstration.

La Chine, quant à elle, est à la tête du WG7 sur les communautés d'information. Les travaux de ce groupe de travail comprennent la normalisation des schémas d'application dans des domaines spécifiques (par exemple, le modèle du domaine de l'administration des terres ou l'occupation des sols). Le groupe de travail aborde également des questions relatives aux métadonnées pour la description des ressources d'information géographique (données et services), aux ontologies afin de soutenir le Web sémantique, et à l'adressage en tant que mécanisme de géoréférencement des entités géographiques. Il est à noter que la norme 19152 modèle du domaine de l'administration des terres (LADM) qui porte sur la création d'une classification normalisée des modes d'administrations de terres, et qui vise à répondre à un besoin exprimé par l'ONU concernant un modèle de donnée internationalement reconnu sur l'administration des terres, divisé en six parties (fondamentaux, Enregistrement foncier, géorégulation des espaces marins, information sur la valeur, Informations sur

[257] Sophia Queret, « Rapport de la Commission AFNOR/CN INFO GÉO - Information géographique et systèmes géodésiques - juillet 2023 - septembre 2024 », 2023.

les plans d'occupation des sols, Aspects liés à la mise en œuvre) est développé au sein du WG7. Cette norme est d'une importance toute particulière pour la Chine, qui s'est investie largement dans la rédaction de la partie numéro trois de cette norme concernant la géorégulation des espaces marins. Avec les nombreuses disputes territoriales, en particulier en mer de Chine du Sud à laquelle la RPC s'est retrouvée mêlée ces dernières années, l'intérêt prononcé des représentants chinois pour une norme visant à réguler la façon dont les espaces marins sont délimités, notamment concernant la souveraineté des États sur ces derniers a attiré l'attention de nombreux experts en normalisation.

L'ISO/TC 211 a publié 89 standards, et 28 autres sont en préparation. Les standards de l'ISO/TC 211 sont tous fondés sur le même modèle, encodé en UML (Unified Modelling Language). Cela signifie que l'ensemble de ces standards sont des branches d'un modèle global pour l'information géographique. L'existence d'un modèle global signifie essentiellement que chaque norme individuelle est connectée de manière logique et harmonisée avec le reste des normes. Une caractéristique commune à toutes les normes ISO est le principe « Un terme - une signification », qui est valable dans l'ensemble du monde des normes ISO. Ce principe a permis de créer et de maintenir une terminologie très stable dans le domaine de l'information géographique.

Les normes publiées par l'ISO sont approuvées par de nombreux pays et jouissent donc d'une large reconnaissance à l'international. L'ISO, en tant qu'organisme de gestion, garantit la stabilité à long terme des normes. La terminologie est cohérente dans l'ensemble du monde de l'ISO. Un des enjeux clés est de maintenir une coopération fructueuse entre la normalisation ISO et les travaux de L'Open Geospatial Consortium (OGC) Les normes ISO 19100 constituent une base stable pour de grands projets, tels que le Geography Markup Language (GML) écrit en XML.

1.1.2 La France au sein de l'ISO

La France est un acteur historique de la normalisation internationale. Elle fait partie, aux côtés d'autres pays européens, comme l'Allemagne et le Royaume-Uni, des pays les plus actifs sur la scène internationale en matière de normalisation. Comme indiqué précédemment, au sein de l'ISO, les comités techniques (CT) et leurs sous-comités sont au cœur du processus de normalisation. Comme l'indique l'AFNOR, *« assurer un secrétariat de comité technique ou de sous-comité est un signe d'influence en normalisation internationale »*[258]. Cela traduit la faculté d'un membre à s'impliquer davantage et à mobiliser des ressources sur le long terme, pour en retour renforcer sa capacité à mener les débats, tant sur le plan technique que stratégique. Le nombre de secrétariats constitue donc

[258] AFNOR, « Baromètre international 2021 », 2021.

l'indicateur retenu par la plupart des pays pour mesurer et comparer leur poids en normalisation internationale. L'évolution de cet indicateur est également observée de près, car l'obtention de nouveaux secrétariats est souvent le signe d'une activité innovante et d'une attitude proactive. L'étude de l'influence d'un Membre dépasse toutefois cette seule variable et s'apprécie aussi à l'aune de son implication dans chaque type de structures techniques, du groupe de travail au comité technique.

La France se place troisième en nombre de secrétariats internationaux, tant à l'ISO qu'à l'IEC[259]. Six pays se démarquent par le grand nombre de secrétariats de comité technique qu'ils occupent : l'Allemagne, les États-Unis, la France, le Royaume-Uni, le Japon et la Chine. L'Allemagne se distingue clairement du reste du monde, en cumulant près de 18 % des secrétariats de comité technique et de sous-comité pour le monde entier. Les États-Unis se placent en deuxième position avec 13 % des secrétariats. La prédominance américaine dans les instances internationales de normalisation n'est pas nouvelle, mais cette réalité ne doit pas faire oublier le retrait progressif des Américains de la scène internationale, constant depuis 2014[260]. Ce retrait de la présence américaine est généralement interprété comme la montée d'une certaine méfiance envers le multilatéralisme, accentué sous la présidence Trump. De plus, la normalisation américaine reposant entièrement sur l'implication d'acteurs privés, cette dernière enregistre souvent de plus fortes fluctuations, en fonction de l'implication de ces sociétés, que dans d'autres systèmes, où l'État joue un rôle plus important dans l'impulsion d'une politique globale de normalisation. Cependant, depuis 2019, les instances américaines en charge des études portant sur la place de la Chine dans l'économie mondiale ne manquent pas de souligner l'importance de la normalisation dans la stratégie économique chinoise, et le danger pour l'industrie US que représente un retrait américain dans ce domaine[261] . Il faut donc s'attendre à un potentiel retour en force des États-Unis sur la scène internationale, si l'implication chinoise continue d'être perçue comme une menace de premier plan. Cependant, en 2023, ce rebond ne s'est toujours pas matérialisé, ce qui ne manque pas d'inquiéter nombre de leurs partenaires, notamment européens, qui redoutent que ce retrait se fasse aux dépens des acteurs proches des intérêts occidentaux.

Ainsi, la France, en troisième, position se place légèrement devant le Royaume-Uni et le Japon en contrôlant 11,1 % des secrétariats de CT et de sous-comités (contre 10,9 % pour le R-U et 10,4 % le Japon). Enfin, la Chine arrive en sixième position avec 10 % des secrétariats et sous-comités. Ce classement international souligne bien une réalité du leadership mondial en matière de normalisation,

---

259 AFNOR, « Baromètre international 2023 », 2023.

260 Dong Geunh Choi et Erik Puskar, « A Review of U.S.A. Participation in ISO and IEC, Standards Coordination Office Laboratory Programs », National Institute of Standards and Technology, U.S. Department of Commerce (NISTIR 8007), juin 2014.

261 United States Trade Representative, « 2019 Report to Congress On China's WTO Compliance », mars 2020.

qui est l'existence d'un fort déséquilibre en matière de poids économique entre les principaux acteurs et leur poids relatif au sein des instances internationales de normalisation. De fait, l'Allemagne, mais également la France et le Royaume-Uni, sont représentée de façon disproportionnée au sein de l'ISO et de l'IEC par rapport à leur poids économique respectif. Au contraire, la Chine reste sous-représentée par rapport à son poids économique réel. Le regain d'implication de la Chine dans la normalisation internationale depuis le début des années 2010 traduit une inflexion stratégique délibérée, analysée notamment par John Seaman dans sa note pour l'IFRI[262]. Cette inflexion repose sur deux axes complémentaires : une réforme profonde de l'architecture normative nationale, conduisant à une rationalisation des instances de normalisation chinoises[263], et une mobilisation accrue des experts chinois au sein des comités techniques internationaux[264]. Ce double mouvement reflète la prise de conscience, au sein du gouvernement de la RPC, que la maîtrise des standards constitue un levier essentiel de compétitivité industrielle à l'échelle mondiale.

La légère contraction du nombre de secrétariats chinois à l'ISO/IEC en 2020, passant de 79 à 69, soit la première baisse enregistrée depuis quinze ans, ne doit pas être interprétée comme un désengagement. Elle s'explique par une révision des règles de gouvernance de l'ISO portant sur les co-secrétariats, mécanisme que la Chine avait largement mobilisé au cours des années précédentes pour acquérir une présence rapide dans des structures techniques où son expertise était encore limitée. En adossant ses candidatures à des membres disposant d'une expérience plus ancienne, la délégation chinoise avait pu, dès 2017, obtenir via ce dispositif près du tiers de l'ensemble de ses responsabilités à l'ISO. La normalisation des règles encadrant ce mécanisme à la fin de la décennie 2010 a mécaniquement entraîné une réduction de ces positions. Sans surprise, depuis 2021, la Chine a de nouveau augmenté son nombre de secrétariats. Si la tendance actuelle se poursuit entre Américains et chinois, on peut d'ores et déjà envisager un croisement des courbes à l'horizon 2024 concernant le nombre de secrétariats occupés par ces deux pays. La France, elle, continue de progresser en termes de nombre de comités et de sous-comités, comme tous les ans depuis 2017. Ainsi, en 2022, la France a de nouveau augmenté son nombre de secrétariats avec la création d'un comité technique sur les stations de ravitaillement en gaz naturel.

Ce classement révèle également une surreprésentation occidentale, qui trouve ses racines à la fois dans l'Histoire de la normalisation internationale et dans l'industrialisation précoce des pays

[262] Seaman John, *China and the New Geopolitics of Technical Standardization*, Notes de l'IFRI, Paris, Institut français des relations internationales, janvier 2020.
[263] Ping Wang et Zheng Liang, « Beyond Government Control of China's Standardization System History, Current Status and Reform Suggestions », EWC-NSF workshop Mega Regionalism – New Challenges for Trade and Innovation (MCTI), Honolulu, 27 janvier 2016.
[264] Rühlig Tim, « China, Europe and the New Power Competition over Technical Standards », *The Swedish Institute of International Affairs*, 2021.

occidentaux. Une situation contre laquelle l'ensemble des comités techniques de l'ISO cherchent à lutter, à travers diverses initiatives visant à favoriser l'entrée de pays en développement au sein de leurs comités. Ainsi, le système de jumelage mis en place par l'ISO et l'IEC a été remanié en 2019 pour le recentrer sur sa fonction première, qui est d'aider la montée en compétence des pays en développement.

Après avoir examiné la gouvernance des comités techniques, il est également nécessaire de se pencher sur celle des groupes de travail, qui sont en charge de la rédaction des normes. Les activités de ces groupes sont conduites par un animateur, qui est un expert nommé par un des membres du comité technique auquel le groupe de travail est subordonné. Comme pour les comités techniques, les mêmes six pays sont en tête concernant la gouvernance des groupes de travail. Les États-Unis occupent ici la première place avec 18 % des groupes de travail, devant l'Allemagne (15 %). Viennent ensuite la Chine (11,5 %), le Royaume-Uni (9,15 %), puis le Japon et la France avec 9,7 et 8,3 % des groupes de travail respectivement. Les groupes de travail dont la France a pris la tête en 2022 sont le reflet des intérêts français en matière de normalisation. Parmi ces dix nouveaux secrétariats, on peut noter la norme sur la gouvernance digitale (ISO/TC 268/SC 2/WG 1), ainsi que celui sur les services spatiaux en aval et applications spatiales (ISO/TC 20/SC 14/WG 8). Autant de travaux qui reflètent l'importance pour la stratégie française en matière de normalisation des problématiques de cybersécurité et des technologies spatiales, intimement liées aux données géographiques.

Afin de mesurer correctement le niveau d'engagement des différents pays au sein de ces groupes de travail, il est nécessaire de retenir la différence entre les membres participants (P) et les membres observateurs (O). Les premiers s'engagent à participer aux réunions et peuvent nommer des experts dans les groupes de travail, ils doivent également s'engager à voter sur tous les documents normatifs du comité technique et du sous-comité. Les membres observateurs, eux, se contentent d'assurer une veille, ne votent qu'à titre consultatif et ne peuvent pas participer aux groupes de travail. Occuper un poste de membre observateur peut être utile afin de garder un œil sur le développement d'une norme sans avoir à investir trop de temps et de moyen en participant à des groupes de travail. On peut ainsi observer plusieurs approches en fonction des pays. Le Royaume-Uni, l'Allemagne et la Chine s'inscrivent comme membres P dans plus de 95 % des comités techniques et sous-comités auxquels ils participent. La Chine allant même jusqu'à être membre P de 99 % des comités techniques auxquels elle participe. Au contraire, la France, les États-Unis et le Japon ont une approche plus équilibrée. Ils restent cependant membres P dans l'écrasante majorité des comités techniques (85 % pour la France). Le retrait progressif des États-Unis sur la scène internationale se répercute également sur leur participation en tant que membre P, en baisse quasi constante depuis 2015. Sur les sept

nouveaux comités lancés en 2022, la France en dirige un, l'ISO/TC 340 sur les stations de ravitaillement en gaz naturel pour véhicules.

Occupant la troisième position mondiale au sein de l'ISO en termes de comités techniques, la place de la France sur la scène internationale de la normalisation est impressionnante. Au même titre que la position de l'Allemagne et du Royaume-Uni, cette situation confirme la main mise européenne sur les organes internationaux de normalisation dont ils ont été, avec les États-Unis, les fondateurs. Cette situation est régulièrement critiquée par certains États, qui ont des difficultés à s'insérer dans les organismes de normalisation internationaux, comme la Chine. Cette critique de la surreprésentation européenne, et plus largement occidentale, n'est pas sans rappeler les critiques adressées au Conseil de sécurité de l'ONU. Reste que la prédominance européenne a poussé certains acteurs, longtemps après la constitution de l'ISO, à continuer à considérer les normes comme des outils avant tout dédiés au protectionnisme, sans chercher à s'insérer dans les logiques internationales de normalisation. Là encore le cas de la Chine est symptomatique de cette attitude. La participation mondiale au sein de l'ISO dessine donc un espace international de la normalisation très polarisé et inégal, où l'on ne peut s'empêcher de noter la quasi-absence du continent africain et sud-américain.

Aujourd'hui seuls le Japon, qui a investi massivement dans la normalisation internationale aux côtés des États occidentaux dès la fin de la Seconde Guerre mondiale, et la Chine, dont l'arrivée fracassante sur la scène internationale de la normalisation est plus tardive, contestent le leadership occidental sur la normalisation mondiale. Ces deux États ont connu des développements industriels fulgurants dans la seconde moitié du vingtième siècle, mais ont abordé leur implication dans la normalisation internationale différemment. Là où le Japon a immédiatement appuyé son développement technologique et industriel sur de nombreux normes et brevets reconnus internationalement, notamment dans les domaines de la robotique et des hautes technologies, tout en appuyant leur base industrielle sur la sous-traitance via d'autres économies moins développées d'Asie du Sud-Est, la Chine a choisi une voie différente. Forte d'un impressionnant marché intérieur, le développement industriel chinois s'est avant tout reposé sur le protectionnisme économique et son attitude vis-à-vis de la normalisation internationale a reflété cette décision. Cependant, depuis la fin des années 2000, la Chine est revenue sur le devant de la scène concernant la normalisation. De fait, le ralentissement de son économie a mis à jour de nombreuses failles concernant la compétitivité des produits chinois, en particulier concernant les hautes technologies. La Chine s'est installée en quelques années à la sixième place de l'ISO et ne cesse de progresser dans ce classement, en s'appuyant sur les investissements massifs du PCC dans la formation et la participation de ses experts en normalisation, une méthode que peu d'États peuvent se targuer de pouvoir égaler. Il est frappant de constater que les deux seuls États non occidentaux qui ont su défier la domination occidentale en matière de

normalisation sont deux économies est-asiatiques qui se sont développées dans des conditions très particulières, que peu d'États dans le monde peuvent espérer pouvoir reproduire, qu'il s'agisse du modèle japonais ou chinois. A contrario l'investissement américain dans la normalisation internationale ne cesse de faiblir ces dernières années. Ce retrait amorcé depuis l'année 2015 semble se confirmer un peu plus chaque année depuis lors. Si on peut y voir un reflet du retrait politique abordé sous la présidence Trump, cela peut également indiquer les limites du modèle ultra libéral choisi par les États-Unis en matière de normalisation. En effet les États-Unis s'appuient uniquement sur le développement de consortiums industriels nationaux pour créer des normes. L'ANSI ne sert qu'à centraliser les propositions de normes que les acteurs industriels américains veulent voir proposer à l'ISO et à porter la voix de ces mêmes acteurs durant les négociations qui y prennent place. Ainsi, ces dix dernières années ont été marquées par un recul progressif des investissements des sociétés américaines en matière de normalisation que les incitations de l'ANSI ne semblent pas prêtes à combler. Si cette tendance continue sur cette voie, la position américaine s'en retrouvera inévitablement affaiblie, mais un retour en grâce de la normalisation n'est pas à exclure selon la volonté de ces sociétés. Avec la montée en puissance de la Chine, nombreux sont les observateurs occidentaux à attendre un sursaut américain en la matière. Enfin, le contrôle des comités techniques est un bon indicateur de l'implication d'un pays, il est également nécessaire de regarder quels pays occupent des postes à responsabilité au sein des instances gouvernantes de l'ISO pour mieux cerner quels États pèsent sur les stratégies normatives internationales.

1.1.3 Les enjeux de la gouvernance de l'ISO

Participer à la gouvernance de l'ISO est un enjeu crucial dans la défense des intérêts français : c'est à ce niveau que sont débattues les orientations stratégiques pour les années à venir, les questions financières, les règles de fonctionnement du système et celles de rédaction des normes, autant de sujets avec des conséquences importantes sur la réalité des travaux de normalisation. Au plus haut niveau de l'ISO se trouve l'Assemblée générale (AG). Cependant, de nombreuses fonctions sont déléguées à d'autres instances qui sont élues par les membres de l'AG.

Au sein de l'ISO, la gouvernance est divisée en deux domaines. Tout d'abord, la gouvernance politique, qui est en charge des sujets, tels que la gestion des ressources financières, la révision ou l'établissement des statuts, les questions juridiques, les orientations stratégiques, ou encore les partenariats avec d'autres organisations. Ces décisions sont du ressort du Conseil de l'ISO. Le Comité du président, qui rassemble le Président, le Vice-Président, le Trésorier et le Secrétaire général, à la

responsabilité de la mise en œuvre de ces décisions d'ordre politique. Enfin, la gouvernance dite technique concerne le fonctionnement quotidien de la normalisation internationale. Elle est exercée par le Bureau de gestion technique (TMB). Cette instance est responsable de la cohérence de la collection des normes et des travaux de normalisation, de la création et de la dissolution des structures techniques, de la gestion des règles de fonctionnement de la normalisation, de l'instruction des conflits envers ou entre les comités techniques, ou encore de la prospective sur des sujets innovants. Il existe un lien étroit entre l'implication dans des travaux techniques d'une part, et la présence et l'influence au sein de la gouvernance d'autre part. Les Membres les plus actifs, qui sont aussi ceux acquittant le niveau le plus élevé de cotisation, sont membres permanents des instances de gouvernance. La place de la France dans l'ensemble de ces instances est également confortée par le nombre important de structures techniques dont elle a la responsabilité.

Si l'Assemblée générale est la plus haute instance de gouvernance de l'ISO, concernant la gouvernance politique, le Conseil est le principal organe de décision et de délibération. Le Conseil est composé de vingt membres, élus par les 164 membres de l'ISO. Les six Membres les plus impliqués au niveau des comités techniques et versant la plus forte cotisation sont membres permanents : il s'agit de l'Allemagne, de la Chine, des États-Unis, de la France, du Japon et du Royaume-Uni. Les quatorze autres membres sont élus pour une période de trois ans[265] . En plus du Conseil et de l'AG, il existe trois autres comités sous la responsabilité du Conseil chargés d'élaborer l'orientation politique sur une série de questions stratégiques. La CASCO est en charge d'évaluer la conformité des normes. Le COPOLCO supervise la prise en compte de l'intérêt des consommateurs dans les normes. Enfin, le DEVCO est chargé de soutenir et promouvoir la participation des pays en développement à la normalisation.

En ce qui concerne la gouvernance technique, le Bureau de gestion technique (TMB - Technical Management Board) joue un rôle clé dans la supervision et l'orientation des travaux techniques au sein de l'ISO. Le TMB est chargé de la création et de la gestion des comités techniques, ainsi que de la conception des règles d'élaboration et de rédaction des normes ISO. Composés de quinze membres élus par le Conseil de l'ISO, seuls les membres assurant au moins une responsabilité au sein d'un comité technique ou d'un sous-comité sont éligibles. Comme pour le Conseil, les membres du TMB sont choisis parmi des groupes de pays classés en fonction de leur implication technique et de leur poids économique, reflétant ainsi la diversité de l'ISO. Les six pays les plus actifs sont membres permanents, tandis que les neuf autres membres sont élus pour un mandat de trois ans, renouvelable une fois[266] .

---

[265] En 2023, les Membres non permanents du Conseil de l'ISO sont les suivants : Afrique du Sud, Australie, Belgique, Bolivie, Brésil, Costa Rica, Danemark, Égypte, Kenya, Inde, Italie, Malaisie, Turquie, Zimbabwe.

[266] En 2023, les Membres non permanents du TMB de l'ISO sont : Argentine, Australie, Brésil, Canada, Corée du Sud, Inde, Malaisie, Norvège, Suisse.

Les sièges des différentes instances gouvernementales de l'ISO sont répartis sur tous les continents. Cependant, le continent africain présente toujours très peu de pays participants, et certaines régions, comme le Moyen-Orient, l'Asie centrale ou l'Amérique centrale, en compte également extrêmement peu, voir aucun. Il faut également noter que, depuis 2021 l'Amérique latine a renforcé sa présence au sein de ces instances gouvernementales, avec l'entrée de l'Argentine et du Brésil au TMB.

Ainsi, sans grandes surprises, les principales caractéristiques de l'ISO en matière de représentativité se retrouvent autant au niveau de l'occupation des comités techniques que de la gouvernance. On y retrouve donc les six mêmes pays au sein des rôles clés de la gouvernance de l'ISO. Ainsi, la capacité d'investissement de ces pays leur permet non seulement de diriger les travaux de normalisation, mais également les orientations stratégiques de l'organisation internationale de normalisation elle-même. Là encore l'investissement financier fait toute la différence entre les membres permanents et les membres temporaires. L'ISO n'est pas l'ONU et, malgré les efforts sincères déployés par l'ISO pour assurer tant bien que mal la représentation d'un maximum de pays, de par sa nature d'organisation non gouvernementale décentralisée et privé, l'ISO repose avant tout sur la contribution financière de ses membres pour fonctionner. Dans le monde de la normalisation, la capacité financière reste le maître mot pour pouvoir participer efficacement et peser sur les processus de décision. Si les postes temporaires permettent à l'ISO de garantir une représentation élargie et participe indéniablement à attirer l'attention de pays peu actifs dans la normalisation internationale sur les bénéfices que ces derniers pourraient tirer d'un plus grand investissement, il n'en reste pas moins que seuls les postes permanents permettent de mettre en place des stratégies sur le long terme concernant la façon dont la normalisation est organisée à l'échelle internationale. Une nouvelle fois la représentation disproportionnée des pays européens est flagrante et assoit une domination normative sur les technologies futures à rebours de leur véritable poids économique. Cependant, si l'ISO représente les investissements étatiques en matière de norme, pour pouvoir jauger des investissements privés, souvent bien plus conséquents en matière financiers et humains, il faut se tourner vers les consortiums privés. Dans le domaine des informations géographiques, le principal consortium privé est l'Open Geospatial Consortium (OGC) qui rassemble l'ensemble des industriels impliqués dans la normalisation des données géographiques.

1.2 L'Open Geospatial Consortium (OGC)

Les organismes de normalisation étatiques interagissent également de plus en plus avec des consortiums privés développant des normes dans le même domaine. Concernant la normalisation des données géographiques, l'Open Geospatial Consortium (OGC) représente le plus important consortium privé qui, en 2023, compte plus de 500 membres, plus de 80 standards publiés et une centaine de groupes de travail. Le rapprochement entre organismes de normalisation internationaux et consortiums a pour avantage de renforcer la réactivité des normes aux besoins du marché. Un consortium se définit comme une combinaison ou un groupe d'organisations formées pour entreprendre un objectif commun qui dépasse les ressources ou les capacités d'une seule organisation. L'OGC a été créé pour fournir un forum de collaboration et de consensus pour la discussion et la résolution des problèmes d'interopérabilité dans le domaine géospatial. Le travail du consortium est basé sur le volontariat. L'OGC rassemblant l'ensemble des acteurs privés d'importance, dans le domaine des données géographiques, il constitue un véritable fer de lance de la normalisation mondiale dans ce domaine. Ainsi, tous les organismes de normalisation internationaux disposent de comité de liaison avec l'OGC, en charge d'assurer une bonne communication entre les acteurs privés et publics de la normalisation des données géographiques. L'Open Geospatial Consortium (OGC) est le plus important consortium industriel international dans le domaine de l'information géographique. Il a été fondé en 1994 et s'est développé à partir des groupes d'utilisateurs GRASS (Geographic Resources Analysis Support System). GRASS était le système d'information géographique développé par l'armée américaine. Aujourd'hui, l'OGC compte 520 membres provenant de 17 nations et répartis en quatre niveaux d'investissement : membres stratégiques (9), membres principaux (17), membres votants (67) et membres associés (427)[267].

Les neuf membres stratégiques comptent beaucoup de grandes entreprises et institutions américaines, telles que la NASA, la NGA (National Geospatial Intelligence Agency), ou encore l'US Departement of Homeland Security. Ils financent environ 60 % du budget global de l'OGC. Les seuls membres stratégiques non américains sont GeoConnections, Natural Ressources Canada, L'Agence Spatiale européenne, l'Ordnance Survey, et le United Kingdom Hydrographic Office (UKHO). Les membres principaux comptent beaucoup de grandes entreprises, telles que Airbus Defense & Space, Amazon, Microsoft, Esri, ou encore Google. On y retrouve également une université indienne ainsi qu'une université chinoise. La présence de ces universités au rang des membres stratégiques de l'OGC dénote d'une forte volonté en Inde et en Chine de lier le monde universitaire au domaine de la normalisation des données géographiques, perçues comme des domaines clés au sein de ces deux

[267] Site officiel de l'OGC https://www.ogc.org/about-ogc/ogc-member-list/

géants asiatiques. Les investissements de ces deux pays en matière de technologie satellitaire et spatiale, ainsi que leur intérêt pour le contrôle de leur très large espace maritime n'est pas étranger à ce besoin de lier recherche universitaire et données géographiques. Il est également à noter que l'IGN et Thales font partie des membres votants, au même titre qu'un grand nombre d'instituts géographiques nationaux. Le DGIWG (Defence Geospatial Information Working Group) est également présent parmi les membres votants, assurant ainsi une liaison vitale entre les développements technologiques de l'OGC et les besoins des acteurs de la défense.

En 1999, l'ISO/TC 211 et l'OGC ont entamé une coopération étroite dans laquelle l'OGC joue le rôle de fournisseur de normes au niveau de la mise en œuvre qui s'inscrivent dans le cadre abstrait défini par les normes de l'ISO. Les activités de l'OGC se répartissent entre les documents de référence et les initiatives du programme d'interopérabilité. Les documents de référence couvrent toutes les normes de l'OGC. Les normes abstraites développées à l'origine par l'OGC ont perdu leur pertinence initiale, car nombre de leurs concepts ont été intégrés dans les normes ISO 19100. Aujourd'hui, les spécifications de mise en œuvre forment la pierre angulaire des normes de l'OGC. Avec les initiatives du programme d'interopérabilité, l'OGC fournit des conseils lors du développement de grands projets de SIG, souvent dans le cadre de coopérations internationales.

L'OGC rassemblant, entre autres, de nombreux développeurs de logiciels SIG, tels que ESRI, le développement de normes approuvées par les principaux acteurs du marché permet de garantir qu'une norme développée en partenariat avec l'OGC, ou dérivé de celle-ci (dans le cas des normes développées par le DGIWG pour les besoins des armées, par exemple), sera compatible avec les logiciels employés par la vaste majorité d'utilisateurs. C'est la raison pour laquelle l'OGC développe principalement des normes d'implémentation, plutôt que des spécifications abstraites, qui sont plutôt du ressort de l'ISO. Cela permet à l'OGC de rester attractif auprès de l'ensemble des acteurs du marché qui voient dans cette organisation un moteur de l'innovation technologique dans le domaine des normes géographiques. S'investir dans les travaux de l'OGC permet alors à ces sociétés de contribuer au développement de standards qui correspondent aux spécificités des logiciels et applications qu'elles développent. Les domaines souvent cités comme pouvant bénéficier d'un rapprochement accru entre consortiums open source et organisations de normalisations sont la cybersécurité, les technologies Internet, le développement de logiciels, le cloud, l'Internet des objets (IoT), la 5G, le Big Data, les technologies géospatiales ou la blockchain[268] .

[268] Justus Baron et coll., « Making the Rules: The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights », TILEC Discussion Paper, Tilburg University, octobre 2019.

1.3 Le World Wide Web Consortium (W3C)

Le World Wide Web Consortium (W3C) a également été fondé en 1994. Il compte 450 membres[269] . Il s'agit d'entreprises du secteur de l'informatique qui développent en commun la technologie d'Internet et les normes qui s'y rapportent. Certaines normes développées par le W3C sont d'une pertinence particulière concernant les informations géographiques :

- XML (Extensible Markup Language) : Comme les documents en XML peuvent être interprétés par tous les navigateurs Internet disponibles, ce langage est devenu le moyen le plus populaire pour transférer des informations sur l'Internet, informations géographiques comprises.
- DTD (Document Type Definition ou définition de type de document) : Il s'agit d'un fichier, ou d'une partie d'un document SGML ou XML, qui décrit ce document ou une classe de documents. Lors de la lecture d'un document XML, un navigateur compare sa structure aux définitions du DTD associée. Toutefois, l'étendue syntaxique d'un DTD présentant certaines limites, d'autres façons de définir la structure d'un fichier XML sont apparues.
- SVG (Scalable Vector Graphics) : SVG est une extension de XML. SVG fournit une grande variété d'éléments graphiques qui permettent la création de cartes de haute qualité. Les données graphiques sont transportées dans un format vectoriel qui permet un affichage à l'écran avec une résolution correcte, quelle que soit l'échelle. Le SVG permet à chaque navigateur Internet de devenir un périphérique de visualisation cartographique.
- SMIL (Synchronized Multimedia Integration Language) : SMIL est également une extension de XML. Le SMIL est capable de définir des éléments animés dans un document. Le SMIL est parfois appelé le « PowerPoint de l'Internet ».

La numérisation des informations géographiques a rendu les travaux du W3C essentiels à la compréhension de l'architecture des normes concernant les informations géographiques. Si son importance n'est pas aussi grande que l'OGC, les normes du W3C constituent les fondations de nombreuses autres normes en matière de traitement de données et d'affichage cartographiques sur lesquelles se reposent les normes développées par l'ISO/TC 211 et l'OGC.

[269] Site officiel du W3C https://www.w3.org/Consortium/Member/List

2. Les acteurs européens

Comme vu précédemment, les acteurs européens jouent un rôle de premier plan dans la normalisation internationale. Si l'ancienneté de leur implication au sein des instances internationales de normalisation explique en partie leur place toujours prépondérante aujourd'hui. Cependant, avec la création de l'Union européenne, du CEN/CENELEC et de l'ETSI, les pays européens ont pu consolider une approche commune de la normalisation et intégré de façon très étroite les normes nationales des différents pays membres et les nouvelles normes approuvées par le CEN. Les lois européennes se surimposant aux lois nationales, les normes approuvées par les organes européens de normalisation s'imposent à tous les pays membres, permettant une uniformisation du marché européen et une fluidification des échanges au sein de l'espace économique européen. Dans l'écosystème international de la normalisation, la capacité des pays européens à faire front commun sur des sujets de normalisation et à défendre leur espace économique constitue une spécificité de l'Union européenne qui explique également la grande résilience des pays européens au sein des espaces de normalisation malgré le recul de leur économie à l'échelle mondiale depuis leur création.

2.1 Un écosystème international marqué par son interdépendance

L'écosystème de la normalisation des données géographiques est marqué par une très forte endogamie de ses membres, et un haut niveau de coopération entre les différents organismes de normalisation. Comme indiqué précédemment les données géographiques sont encore aujourd'hui considérées comme des données de niche, et, à fortiori, le travail de normalisation associé à ces données l'est encore plus. Cette situation aboutit à ce qu'un nombre relativement limité de personnes participent activement à ces travaux de normalisation dans les différents pays et organismes concernés. Ainsi, en France, environ une quinzaine de personnes sont activement engagées dans des travaux de normalisations à l'échelle internationale, et toutes sont des membres de l'IGN. De plus, les individus et les entreprises qui participent à ces processus de normalisation ont chacun leur propre réseau de relations, et ces réseaux sont généralement liés les uns aux autres. La plupart des acteurs qui prennent part à ces processus de normalisation sont membres de plusieurs organismes de normalisation, un état de fait qui renforce la circulation de l'information et l'interaction entre ces différents organismes. Les relations qu'entretiennent entre eux ces différents organismes peuvent être de nature hiérarchique ou plus horizontale.

À l'échelle internationale, l'ISO est considéré comme l'organisme de référence en particulier pour les acteurs étatiques, et tire sa légitimée à la fois de son ancienneté et de ses liens historiques avec les autres grands organismes internationaux de normalisation, tels que la Commission électrotechnique internationale (CEI) et l'Union internationale des télécommunications (UIT). Ce système global est lié,

« par des accords de collaboration entre l'ISO, la CEI et l'UIT au niveau international, et par des accords similaires, entre les organisations de normalisation au niveau régional, tel que le CEN, le CENELEC et l'ETSI en Europe, et à la base, par un large éventail d'accords de collaboration entre les membres nationaux des trois organisations majeures »[270].

Au niveau européen, la même vision hiérarchique est reproduite au niveau régional. Le système de normalisation européen est un des plus gros producteurs de nomes au monde, avec comme objectif affiché la suppression des entraves techniques aux échanges dès les années 1960. Aujourd'hui l'Union européenne compte près de 200 000 experts et 620 comités techniques et environ 20 000 normes disponibles. Grâce à la combinaison des lois de l'UE et des communications de la Commission européenne, un modèle de gouvernance des organismes européens de normalisation est établi, qui suit de près le modèle international mentionné au paragraphe précédent. Les organismes européens de normalisation (CEN-CENELEC et ETSI) incarnent ce modèle de gouvernance. Le CEN, établi en 1961 et ayant son siège à Bruxelles, a la responsabilité de développer des normes dites « générales »[271] et est compétent pour la normalisation de produits, de matériaux, de services ou de procédés qui ne sont pas de la compétence d'organismes plus spécialisés tels que le CENELEC et l'ETSI. Il se compose de 34 organismes membres, parmi lesquels figurent les 27 États membres de l'Union européenne, ainsi que la Suisse, le Royaume – Uni, l'Islande, et la Norvège. De plus, trois États candidats à l'adhésion à l'Union européenne, à savoir la Turquie, la Macédoine du Nord et la Serbie, font également partie de ses membres. Tous ces membres jouissent du droit de vote dans toutes les procédures du CEN. Le CENELEC, dont le siège se trouve à Bruxelles, a pour mission de superviser les activités de normalisation européenne dans le secteur de l'industrie électrotechnique. Il est composé de 34 organismes issus des États membres européens, dont les 28 États membres de l'Union européenne. De plus, il compte 12 membres affiliés originaires d'Europe de l'Est, d'Afrique du Nord et du Moyen-Orient, qui ont un statut d'observateur sans droit de vote.

Les organismes nationaux de normalisation en Europe, tels que l'AFNOR, sont désignés par leurs gouvernements nationaux comme membres du CEN ou du CENELEC, et sont soumis aux exigences d'adhésion du CEN-CENELEC. Le règlement intérieur du CEN-CENELEC définit des

[270] Guide ISO/CEI 59:1994, « Code de bonne pratique pour la normalisation », paragraphe 1.2.

[271] Règlement intérieur du CEN-CENELEC Partie 1:2022 : Organisation et structure. Partie 1D : Exigences applicables aux Membres du CEN et du CENELEC.

exigences spécifiques en matière de procédure et des principes concernant l'efficacité, la cohérence et la viabilité que les organismes nationaux de normalisation membres sont tenus d'adopter. Les organismes nationaux de normalisation se tournent donc vers les niveaux régional et international pour obtenir des conseils en matière de gouvernance. Parallèlement, la prise de décision au sein du CEN et de l'ISO est pilotée par ces organismes nationaux. Du fait de cette relation hiérarchique qui lie organismes internationaux et nationaux, la plupart des débats sur la gouvernance et la politique ont lieu au niveau européen ou international.

2.2 La France, un poids lourd des institutions de normalisation européennes

Ainsi, les normes adoptées par l'AFNOR, en matière d'information géographique notamment, sont avant tout le résultat des débats internationaux prenant place à l'ISO et à l'adoption par les organismes de normalisation européens de ces mêmes normes. Outre son rôle d'élaborateur de normes, l'AFNOR a obtenu une reconnaissance juridique de la part du gouvernement français, ce qui lui confère la responsabilité de définir la stratégie nationale de normalisation (transposant souvent des principes internationaux) qui est suivie par de nombreux organismes ou comités sectoriels de normalisation. L'AFNOR contrôle en outre les organismes de normalisation sectoriels français accrédités par le gouvernement français[272] .

Au niveau européen, le CEN-CENELEC et l'ISO coopèrent fréquemment. Les organisations nationales, telles que l'AFNOR et le DIN, coopèrent avec d'autres organisations nationales au sein d'entités régionales ou internationales. Au sein du CEN-CENELEC, par exemple, les organisations britannique (BSI), française (AFNOR) et allemande (DIN) entretiennent des relations de travail étroites. Dans le système européen de normalisation, la coopération l'emporte sur la concurrence.

Lorsque l'on observe l'implication des différents pays européens dans les travaux du CEN-CENELEC, on retrouve la France et l'Allemagne largement en tête du classement. Ainsi, ces deux pays à eux seuls gèrent plus de la moitié des structures techniques de CEN-CENELEC. De fait, l'Allemagne compte à elle seule 32 % des comités techniques, tandis que la France en occupe 23 %. Le Royaume-Uni occupe la troisième place avec seulement 13 % des comités, puis viennent ensuite l'Italie avec 9,2 % et, enfin, les Pays-Bas ferment la marche du top avec 6,6 % des comités[273] . Concernant la gouvernance des comités techniques et sous-comité du CEN, on retrouve la majorité des pays cités précédemment. La France dirige un quart des secrétariats de structures techniques au sein du CEN (25 %), arrivant en deuxième position derrière l'Allemagne (30 %), et loin devant le Royaume-Uni

[272] Décret n° 2021-1473 du 10 novembre 2021.
[273] AFNOR, « Baromètre international 2023 », 2023.

(12 %). Viennent ensuite l'Italie (9,11 %) et les Pays-Bas (8,59 %). La France fait ainsi partie des principaux animateurs du système, qui assurent à eux seuls plus de 80 % des secrétariats. Sept autres membres occupent plusieurs responsabilités techniques : la Suède (4 %), l'Espagne (3 %), la Suisse (2 %), la Belgique (2 %), la Norvège (2 %), l'Autriche (1 %) et le Danemark (1 %). Le reste des pays de l'Union sont significativement moins impliqués dans les processus de normalisation européens, n'occupant qu'un ou deux secrétariats, voir aucuns. Enfin, concernant les secrétariats de groupes de travail au sein du CEN, la France occupe également la deuxième place, avec 17 % des secrétariats de comités techniques et sous-comités. L'Allemagne arrive de nouveau première avec 32 %, tandis que le Royaume-Uni occupe la troisième place avec 11 %. Viennent ensuite les Pays-Bas (6,4 %), l'Italie (6,1 %), la Suède (3 %), la Belgique (3 %) et le Danemark (2 %).

Une des grandes forces de l'Union européenne en termes de normalisation est sa très forte intégration, puisque la préséance des règlements européens sur les règlements nationaux permet l'adoption obligatoire des normes européennes dans les pays membres, et le retrait automatique de normes nationales contradictoires. Cela garantit l'uniformisation du tissu normatif européen dans tous les domaines techniques.

Comme pour l'ISO, la gouvernance des instances décisionnelles du CEN est au cœur des enjeux de pouvoir au sein des institutions de normalisation européennes. Cette dernière est également divisée entre gouvernance politique et gouvernance technique. La première est exercée par le Conseil d'administration (CA) du CEN, la seconde est gérée par les Bureaux techniques (BT). Tout d'abord, le CA compte 13 membres chargées de protéger les intérêts de l'association. Le Président est accompagné dans cette tâche par trois Vice-Présidents. Les membres du CA sont répartis en quatre groupes selon leur PIB et leur population. Ils sont élus par l'Assemblée générale. Chaque membre est élu pour un mandat de deux ans. Les quatre Membres du premier groupe, les plus impliqués dans les travaux de normalisation, l'Allemagne, la France, l'Italie et le Royaume-Uni, sont représentés de manière permanente[274] . Les trois réunions annuelles des CA du CEN et du CENELEC se tiennent au même moment, afin de tenir ensuite une session commune, où les sujets transverses peuvent être débattus, garantissant une prise de décision commune. En termes de gouvernance, l'année 2021-2022 a été marquée par un net renforcement de l'influence française, avec la nomination de Olivier Peyrat, directeur général de l'AFNOR, à la vice-présidence politique du CEN[275], et celle de Frédéric Vaillant à la vice-présidence technique du CENELEC[276]. Il faut également noter qu'en 2022, la France a pris la

[274] Au 1er janvier 2023, les autres Membres nationaux formant le Conseil d'administration du CEN sont les suivants : Chypre, Espagne, Finlande, Irlande, Lettonie, Norvège, Suède, Suisse.

[275] AFNOR, Communiqué de presse, « Olivier Peyrat, directeur général d'AFNOR, est nommé vice-président « elect » en charge des questions politiques du Comité européen de normalisation (CEN) », 21 juin 2021.

[276] Site officiel du CENELEC : https://www.cencenelec.eu/about-cenelec/structure-and-governance/cenelec-board-members/

tête de la présidence tournante de l'UE, contribuant à mettre en lumière les sujets portés par la France au niveau européen.

Enfin, concernant la gouvernance technique, ce sont les Bureaux techniques (BT) qui en ont la charge. Ces derniers sont notamment responsables de la création de nouveaux domaines d'activité, de la bonne gestion des travaux techniques, ainsi que de la gestion des règles d'élaboration et de rédaction des normes. Les Bureaux techniques du CEN et du CENELEC sont composés de représentants issus de l'ensemble des organismes de normalisation membres, mais également d'observateurs venus d'autres organisations. On y retrouve notamment des organisations professionnelles à caractère sectoriel, telles qu'Orgalim[277] et la FIEC[278], mais également des organisations représentant les parties prenantes sociétales (ANEC[279] pour les consommateurs, ECOS[280] pour les associations environnementales et ETUC[281] pour les syndicats de salariés) ainsi que les PME (SBS)[282]. On compte aussi d'autres organisations européennes ou internationales de normalisation, telles que l'ETSI, l'ISO ou l'IEC, ainsi que la Commission européenne (CE) et l'Association européenne de libre-échange (AELE). À ces réunions s'ajoutent, pour le CEN, deux réunions annuelles du groupe du BT pour la gestion des comités techniques (Technical Committees Management Group - BT/TCMG), dont la présidence est allemande. Par délégation, celui-ci prend les décisions sur les activités opérationnelles des structures techniques. Y participent de facto les Membres assurant des secrétariats, dont la France.

Il existe également une structure commune à la fois au CEN et au CENELEC, le Centre de gestion du CEN et du CENELEC (CCMC), qui dispose d'une instance de pilotage et de coordination, le Comité présidentiel. Ce dernier est en charge d'examiner les sujets stratégiques d'intérêt commun aux deux organisations, comme les demandes d'adhésion de nouveaux Membres, les relations entre instances européennes et internationales, la représentation des intérêts sociétaux, ainsi que l'innovation et la recherche. Le Comité présidentiel est composé de neuf membres : les Présidents du CEN et du CENELEC, qui sont généralement élus par les Assemblées générales parmi les parties prenantes, les Vice-Présidents de chacune des organisations pour les questions politiques, techniques et financières (élus par les Assemblées générales parmi les membres de leur Conseil d'administration respectif), ainsi que la Directrice générale du CEN et du CENELEC (qui assure le secrétariat).

Au sein des instances de la gouvernance européenne, le couple franco-allemand domine largement en occupant à eux seuls plus de la moitié des comités techniques. Avec la nomination de deux représentants français aux instances de gouvernances du CEN et du CENELEC en 2022, la France

277 Association européenne des industries d'ingénierie (Orgalim).
278 Fédération européenne de l'industrie de la construction (FIEC).
279 Association européenne pour la coordination de la représentation des consommateurs dans la normalisation (ANEC)
280 Organisation citoyenne environnementale européenne pour la normalisation (ECOS)
281 Confédération européenne des Syndicats (ETUC)
282 Small Business Standards (SBS).

a renforcé sa position déjà dominante au sein de la normalisation européenne. Le maintien de la France comme force de proposition au sein des instances européennes est une part importante de la réussite de la stratégie nationale de normalisation en participant du maintien de son leadership à l'échelle européenne. Cette échelle géographique est capitale pour le maintien de la place de la France au sein des instances internationales de normalisation du fait de la préséance des lois européennes sur les lois nationales. Ainsi, seul le maintien d'une capacité de négociation forte au sein des instances européennes peut permettre à la France de faire porter sa voix à l'échelle internationale en s'appuyant sur le vaste réseau des experts européens dont le soutien est essentiel à l'ISO. De plus, la consolidation d'un espace normatif européen aligné avec les intérêts français protège également les sociétés françaises en permettant le développement de normes qui leur sont favorables. L'unicité du marché européen assure également aux sociétés européennes de disposer d'un poids bien plus important au sein des consortiums privés de normalisation, tels que l'OGC. En effet, ces sociétés vont pouvoir s'appuyer sur le poids de l'ensemble du marché européen pour pouvoir promouvoir des normes conformes aux intérêts des pays de l'Union. Le CEN et le CENELEC offrent également des espaces protégés de négociations pour le pays membre et contribuent grandement à la qualité des projets de normes européennes portés à l'ISO. Ainsi, il est important que la France continue à investir du temps et de l'argent pour conserver sa place de leader au sein des instances européennes de la normalisation, qui constitue une plateforme essentielle pour la défense des intérêts français en la matière.

2.3 Le renouveau de la stratégie européenne en matière de normalisation de données géographiques depuis les années 2000

Comme le rappelle la Commission européenne dans sa stratégie de 2022, *« les normes sont au cœur du marché unique de l'UE »*[283]. Au cours des trente dernières années, le système européen de normalisation a produit plus de 3 600 normes harmonisées permettant aux entreprises de démontrer leur conformité avec le droit de l'UE, ainsi qu'un nombre bien plus élevé de normes et spécifications techniques européennes visant à promouvoir l'interopérabilité, la sécurité des citoyens de l'UE et la protection de l'environnement. Concernant la normalisation des données géographiques en Europe, elle s'est principalement structurée autour de la directive INSPIRE[284], établissant une infrastructure d'information géographique dans la Communauté européenne, entrée en vigueur le 15 mai 2007. Dès 2004, la Commission avait présenté une proposition de directive INSPIRE axée principalement sur les « données spatiales », c'est-à-dire les informations relatives à un lieu ou à une zone sur Terre[285]. La directive INSPIRE oblige les États membres à partager les données géospatiales dont elles disposent, et ce, *« afin de soutenir les politiques environnementales de l'Union européenne (UE) et les politiques ou activités susceptibles d'avoir un impact sur l'environnement »*[286] *»* La directive INSPIRE s'appuie sur les infrastructures d'information géospatiales déjà établies et exploitées par les États membres, et ne comporte aucune obligation de production de données supplémentaires. Au sein de cette infrastructure, les systèmes d'information existants des différents pays sont connectés afin de partager, de trouver et d'utiliser plus facilement les données géographiques tout en s'appuyant sur des normes de données communes de haute qualité. Pour répondre aux besoins des États membres de l'Union européenne, les données doivent être comparables et utilisables dans un contexte transfrontalier et intersectoriel. Le besoin de normalisation de ces données, et la constitution d'un espace européen de données est donc au cœur du projet de la directive INSPIRE. De plus, la directive INSPIRE a été transposé sur le plan législatif par l'ordonnance n°2010-1232 du 21 octobre 2010[287], ratifiée par la loi n°2011-12 du 5 janvier 2011[288]. L'ordonnance a conduit à ajouter au code de l'environnement un chapitre intitulé « De l'infrastructure d'information géographique », introduisant les nouveaux articles L. 127-1 à L. 127-10

---

283 Commission européenne, « Une stratégie de l'UE en matière de normalisation » ,COM(2022) 31 final, 2 février 2022, p.1

284 Directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE).

285 L'article 3 de la directive INSPIRE, définie les "données géographiques" comme : "toute donnée faisant directement ou indirectement référence à un lieu ou à une zone géographique spécifique". Par exemple, les données spatiales peuvent être un polygone dont les coordonnées définissent les limites d'un site protégé, les limites d'un site industriel, d'une installation. Mais il peut également s'agir de données collectées sur des espèces présentes dans un site protégé et référencées par rapport à celui-ci ou de mesures prises par un capteur au point d'émission, de données administratives relatives à une installation industrielle ou de données statistiques relatives à la zone géographique d'une unité administrative.

286 Document de travail des services de la Commission résumée de l'évaluation de, La DIRECTIVE 2007/2/EC établissant une infrastructure d'information spatiale dans la Communauté européenne (INSPIRE)., Bruxelles, 13 juillet 2022.

287 Ordonnance n° 2010-1232 du 21 octobre 2010 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière d'environnement, 21 octobre 2010.

288 Loi n° 2011-12 du 5 janvier 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne, 6 janvier 2011.

dans ce code. Dans le cadre de la mise à disposition de données appartenant à un grand nombre de pays différents, la normalisation des jeux de données joue un rôle capital. Ainsi, l'architecture orientée services qui a été conçue pour mettre à disposition des outils de visualisation de ces données est fondée sur des normes de l'Open Geospatial Consortium pour l'interopérabilité géospatiale. Les métadonnées sont publiées à l'aide des services de découverte INSPIRE via la norme Catalog Service for the Web (CSW), les services de visualisation INSPIRE sont basés sur les normes Web Map Service (WMS) et Web Map TileService (WMTS), et les services de téléchargement INSPIRE sont basés sur les normes Web FeatureService (WFS), Web Coverage Service (WCS) et Sensor Observation Service (SOS) conçu par l'OGC.

L'application de la directive INSPIRE s'inscrit également dans la stratégie européenne globale en matière de de données numériques dévoilées par une Communication de la Commission en février 2020[289]. Un des principaux piliers de cette nouvelle stratégie est la nouvelle stratégie européenne pour les données, annoncé en même temps[290]. La stratégie européenne pour les données définit une vision à l'échelle de l'Union pour allier transition écologique et économie numérique. Cette dernière insiste également sur la nécessité de diffuser au maximum les données pour le bien public. La nouvelle stratégie européenne souligne les avantages liés au partage des données au sein de l'économie numérique, ainsi que son utilité pour lutter contre le changement climatique. Ces deux directives ont été conçues afin de garantir l'accès à de meilleures données et informations, et de faciliter leur diffusion à l'ensemble des pays membres, le tout afin de soutenir plus efficacement les politiques de développement de l'Union européenne. Il convient également de citer ici la stratégie de l'UE en matière de normalisation, qui a été publiée par à Commission en février 2022[291]. Cette dernière annonce pour la première fois la mise en place d'une véritable stratégie à l'échelle de l'Union afin de rendre plus compétitive la normalisation européenne au regard de la compétition internationale en matière de normalisation. Au sein de cette nouvelle stratégie, la normalisation des données qui renforcent l'interopérabilité à l'appui des espaces européens communs de données est citée comme une priorité.

L'objectif général de la directive INSPIRE reste la création d'une infrastructure d'information géographique à l'échelle de l'UE, basée sur les infrastructures compatibles des États membres et utilisables dans un contexte transfrontalier au sein de l'Union afin de soutenir les politiques environnementales des pays membres et les politiques ou activités susceptibles d'avoir un impact sur

[289] Rapport de la Commission au Parlement européen, au Conseil et au Comité économique et social européen, « Rapport sur les conséquences de l'intelligence artificielle, de l'Internet des objets et de la robotique sur la sécurité et la responsabilité (COM(2020) 64 final) », Bruxelles, 19 février 2020.

[290] Communication de la Commission européenne de la Commission au parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Une stratégie européenne pour les données », Bruxelles (COM [2022]) 19 février 2020.

[291] La Commission européenne, « Une stratégie de l'UE en matière de normalisation. Définir des normes mondiales à l'appui d'un marché unique européen résilient, vert et numérique », Bruxelles, 2 février 2022.

l'environnement[292]. Le développement d'une telle infrastructure européenne de données spatiales est motivé, entre autres, par les gains économiques offerts par l'ouverture et le partage des données géographiques, en réduisant les coûts pour les administrations des États membres, et offrant de nouvelles opportunités commerciales. Beaucoup d'entreprises utilisent aujourd'hui ces données pour fournir de meilleurs services au public (par exemple en combinant les prévisions météorologiques et la qualité de l'air ou en intégrant des informations sur le trafic en temps réel dans les processus commerciaux, comme la fourniture d'informations sur les chantiers routiers par le biais de la navigation par satellite). Le secteur de l'assurance utilise de plus en plus les données géographiques pour améliorer sa rentabilité en améliorant sa compréhension des risques sur les sites et en vérifiant le contenu des demandes d'indemnisation. De plus, les sociétés immobilières prennent de plus en plus en compte les informations environnementales, par exemple lorsqu'elles déterminent le prix des maisons (par exemple, si elles sont situées dans une zone inondable) et les opérateurs de réseaux de services publics exploitent les données spatiales pour éviter les dommages causés par les travaux d'excavation.

Un autre type de gain identifié par la Commission, est lié à la capacité des utilisateurs à accéder et à exploiter les données nouvellement disponibles à des fins innovantes et originales, qui pourraient conduire à des gains de productivité dans certains secteurs, ou encore à des gains d'efficacité en matière d'application de politiques publiques dans les États membres, mais également à l'échelle de l'Europe tout entière. De plus, l'UE y voit également un gain politique, dans le sens où la mise à disposition des données géographiques pour les citoyens, et leur exploitation dans le cadre du renforcement des politiques publiques, doit conduire à une confiance renforcée de ces derniers dans la démocratie et l'Union. Ainsi, consciente de l'importance stratégique grandissante des normes internationales, la Commission a déposé en février 2022 une proposition de règlement modifiant le règlement (UE) nº 1025/2012 relatif à la normalisation au sein de l'UE, afin de renforcer le poids des organes représentant l'ensemble de la communauté des parties prenantes, contre la place grandissante prise par les multinationales au sein de l'ETSI. Renforcer la participation équitable de l'ensemble des parties prenantes au sein des organismes de normalisation européens doit passer également par le renforcement de la participation des PME qui rechignent souvent à participer par manque de moyens et de temps à consacrer à la normalisation. Dans une tentative de réponse à cette situation, l'article de 6 du règlement (UE) nº 1025/2012, *« prévoit des conditions plus favorables aux PME (libre accès aux projets de normes, accès aux activités des organismes nationaux de normalisation, application de taux spéciaux pour la mise à disposition de normes, etc.) »*[293]. Dans le même esprit, la Commission a

[292] Article 1 de la Directive INSPIRE.

[293] La Commission européenne, « Une stratégie de l'UE en matière de normalisation. Définir des normes mondiales à l'appui d'un marché unique européen résilient, vert et numérique », Bruxelles, 2 février 2022

cherché à renforcer la transparence des instances de gouvernance des OEN en demandant le libre accès aux publications et aux normes à la société civile.

Aujourd'hui la directive INSPIRE est mise à jour et suivie par un groupe de suivi dédié, le groupe de maintenance et d'implémentation d'INSPIRE (Maintenance and Implementation Group : MIG), au sein de la Commission européenne. Établie par la directive INSPIRE, le groupe de travail sur la maintenance et l'implémentation d'INSPIRE, documente les progrès effectués dans l'application de la directive à l'échelle de l'Union. Il est également en charge de faire évoluer les objectifs d'INSPIRE à l'aune des progrès déjà effectués et des difficultés rencontrées afin d'adapter les objectifs de la directive.

Une large partie du travail du MIG se concentre sur les problèmes d'interopérabilité des jeux de données fournies par les différents États membres, en vue de produire des jeux de données paneuropéens, maximisant ainsi la réutilisation des données. La mise en œuvre actuelle d'INSPIRE est encore très hétérogène et n'a donc qu'une capacité limitée de réutilisation transfrontalière et de construction d'ensembles de données et d'applications paneuropéens. Il existe actuellement plusieurs initiatives et projets en cours qui explorent la possibilité d'utiliser directement l'infrastructure INSPIRE pour créer des ensembles de données et des applications paneuropéennes (par exemple, les projets Eurostat, les activités in situ de Copernicus, l'échange de données du SIGC). Tous ces projets ont en commun la nécessité d'une gouvernance spécifique qui engage les fournisseurs de données et étudie les capacités ou les obstacles techniques. La diffusion des résultats et des enseignements tirés de ces activités est également essentielle pour les améliorations futures. Il est important de noter que la priorisation de certains thèmes et ensembles de données spatiales INSPIRE dans le cadre de cas d'utilisation clairs et d'exigences politiques est considérée comme essentielle pour atteindre l'objectif de construction d'ensembles de données paneuropéens et garantir leur réutilisation. En ce sens, la liste prioritaire des séries de données pour la déclaration en ligne, élaborée dans le cadre du programme de travail précédent, s'est déjà révélée utile, mais elle doit être régulièrement mise à jour pour refléter l'évolution des exigences en matière de déclaration ou de la législation. La synchronisation entre les différentes exigences prioritaires et la disponibilité des ensembles de données permettra également de créer des synergies et d'accroître la possibilité de réutiliser les ensembles de données à des fins différentes[294].

En outre, au-delà du champ d'application des initiatives de hiérarchisation en cours (par exemple, le document de la Commission sur les exigences géospatiales et l'activité sur les données prioritaires pour les rapports environnementaux…), la hiérarchisation des données devrait également tenir compte du nouvel agenda politique (par exemple, la stratégie pour la biodiversité, le plan d'action

[294] INSPIRE work program 2021-2024, Action 2.1 Need-driven data prioritisation.

pour l'économie circulaire, le plan d'action pour une pollution zéro…) et des cadres juridiques émergents (par exemple, les ensembles de données de grande valeur dans le cadre de la directive sur les données ouvertes, les espaces communs de données de l'UE…).

Les dernières évaluations de la Directive INSPIRE soulignent globalement la réussite de cette directive et son rôle central au sein de l'architecture des données communes de l'Union européenne, en facilitant l'accès et la dissémination d'un grand nombre de données. Une des principales raisons de ce succès, est le fait qu'a directif ait été bâtie sur des normes internationalement reconnues et largement adoptées[295]. Parmi les principaux mérites de la directive INSPIRE, on peut citer la promotion du partage des données en tant que principe commun, la mise en place d'une structure de gouvernance efficace, l'approfondissement de l'interopérabilité à l'échelle de l'UE, le déblocage des données publiques, l'amélioration de la transparence et la création d'une réserve d'expertise au niveau de l'UE. La quantité grandissante de données disponibles, mais surtout les larges possibilités offertes pour leurs réutilisations à travers d'autres politiques de l'Union (notamment le European Green Deal) ont également beaucoup contribué au succès de la directive INSPIRE. De plus, du point de vue budgétaire, si les coûts associés à l'implémentation de la Directive sont largement portés par les administrations des pays membres, ceux qui ont analysé ces coûts n'ont pas jamais perçu de coût extraordinaire. Aujourd'hui la directive INSPIRE est reconnue internationalement comme un véritable tour de force en matière d'interopérabilité et de réutilisation des données et est cité en exemple dans de nombreux pays, et milieux, notamment militaire[296]. La directive INSPIRE est observé de près également à l'ISO, où il a été décidé lors de la dernière réunion plénière de l'ISO/TC 211 qui s'est tenue à Jeonju, en Corée du Sud du 15 au 19 mai 2023, de créer un groupe ad hoc sur l'apport aux espaces de données de l'UE. Ce groupe vise avant tout à préparer un document décrivant l'utilisation des normes pour permettre la publication d'ensembles de données de grande valeur conformément au prochain règlement de mise en œuvre basé sur la directive sur les données ouvertes, et la mise en œuvre dans les « espaces de données » conformément à la stratégie européenne pour les données.

Cependant tout n'est pas rose pour autant concernant les données spatiales au sein de l'UE. La fourniture de séries de données spatiales et leur intégration dans les statistiques souffrent ainsi de l'absence d'un mandat officiel au niveau de l'UE et d'un manque de coopération entre les organismes responsables dans les États membres. Si la directive INSPIRE a favorisé l'intégration européenne des séries de données spatiales, l'initiative se limite à des thèmes principalement environnementaux et, en

---

[295] Document de travail des services de la Commission, « résumé de l'évaluation de La DIRECTIVE 2007/2/EC établissant une infrastructure d'information spatiale dans la Communauté européenne (INSPIRE). », Bruxelles, 13 juillet 2022.

[296] Lors de son intervention durant la 45e réunion technique du programme MGCP le 26 septembre 2023, un officier du 28e Groupe Géographique à cité INSPIRE comme un exemple de coopération internationale réussi dans le domaine des données géographiques dont devrait s'inspirer les membres du programme de coproduction.

outre, ne prévoit l'intégration qu'en ce qui concerne la structuration et les informations supplémentaires (métadonnées) sur les séries de données. L'élément crucial de l'harmonisation technique de la production de jeux de données spatiales repose toujours sur des lignes directrices non contraignantes. Si les données statistiques bénéficient d'un cadre institutionnel fort et d'une longue histoire en matière de coopération, pour les données spatiales, cela n'est pas encore le cas. Même les éléments obligatoires de la mise en œuvre de la directive sont en retard ou n'ont pas atteint la qualité prévue dans de nombreux États membres. Le processus de mise en œuvre à l'échelle de l'Union n'est pas cohérent, notamment en ce qui concerne la transposition de la directive INSPIRE dans le droit national, qui n'est pas uniforme d'un pays à l'autre, ni les travaux relatifs à l'établissement de services de réseau ou à la coordination et au partage des données. Si le nombre de jeux de données disponible atteint plus de 90 000, un chiffre indéniablement impressionnant, cela ne donne aucune indication sur l'harmonisation de ces données ou leur interopérabilité réelle. Ainsi, l'étude de 2017 a révélé qu'environ un cinquième seulement des jeux de données fournis remplissent les critères d'interopérabilité en termes de métadonnées, ce qui est comparativement faible, étant donné qu'en 2017, les délais pour assurer l'interopérabilité n'avaient pas encore été atteints. Bien que le rapport de synthèse de 2022 sur la mise en œuvre de la directive INSPIRE fasse état de perspectives positives en la matière, la mise en œuvre reste en deçà des objectifs initialement fixés par la directive. Le manque d'interopérabilité concernant des éléments fondamentaux des jeux de données, comme l'application de normes communes, la qualité et l'accessibilité étaient déjà citées comme étant une des causes principales du manque d'efficacité des projets européens reposant sur l'exploitation des données géographiques dans le rapport du Comité européen pour les régions de 2021[297]. D'autres causes sont citées, notamment le manque de communication entre les États membres et une faible interaction entre les différentes agences statistiques nationales. Les données géographiques ont le potentiel d'améliorer de nombreux programmes européens, car elles permettent d'identifier les problèmes avec une résolution beaucoup plus élevée que les données statistiques régionalisées traditionnelles. Cependant, leur utilisation efficace dépend dans une large mesure de l'harmonisation et de l'interopérabilité des ensembles de ces données. Le cadre législatif actuel au niveau de l'UE n'est pas assez strict pour garantir ces points cruciaux, de sorte que les données spatiales sont souvent limitées à des informations complémentaires pour des évaluations qualitatives, ou confinées à de petites zones géographiques où les données sont collectées de manière comparable.

En parallèle de ces initiatives, la Commission européenne a également lancé un ensemble de mesures visant à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de

[297] Roland Gaugitsch et al., « Integration of Geographic and Statistical data for better EU policy making », Commission for Territorial Cohesion Policy and EU Budget, 2021.

l'Union, sous le nom de « Interoperable Europe Act » le 18 novembre 2022[298]. Ce règlement de la Commission vise à mettre en place une série de mesures devant garantir un fort niveau d'interopérabilité au sein des différents services publics des pays membres de l'Union. L'existence de ce règlement souligne bien la prise de conscience au sein des instances européennes de l'importance d'une forte interopérabilité entre ses membres en matière de partage d'informations, et les données géographiques ne font pas exceptions, bien que les résultats en la matière ne soient pas toujours à la hauteur des attentes. L'interopérabilité est également un facteur essentiel pour atténuer les risques croissants de cybersécurité auxquels sont confrontés l'Union et ses États membres. Aujourd'hui, les administrations publiques sont régulièrement la cible de cyberattaques, et l'Union européenne entend renforcer sa résilience en matière de risque cyber par le biais d'un renforcement d'interopérabilité de ses membres, particulièrement concernant le partage des données. Compte tenu de l'environnement réglementaire croissant dans ce domaine, l'Union européenne s'est attelée à la mise en place d'une infrastructure cohérente pour faciliter l'interopérabilité des différents pouvoirs publics. Parmi les exemples de cette règlementarisation croissante, on peut citer la passerelle numérique unique (établie par le règlement UE 2018/1724 du Parlement européen et du Conseil[299], qui met en place une infrastructure technique unique pour l'échange d'informations entre les États membres), et le cadre juridique en évolution autour de l'identité numérique[300], qui établit un cadre aux fins de l'interopérabilité des systèmes nationaux d'identification électronique ou des espaces de données à venir[301]. Les synergies entre les trois directives pourraient toutefois être mieux exploitées. En particulier, INSPIRE peut-être utile pour soutenir davantage la diffusion active d'informations dans le cadre des deux directives susmentionnées[302].

La question de l'interopérabilité du secteur public n'est pas actuellement couverte par des dispositifs politiques contraignants au sein de l'UE. Cependant, le cadre européen d'interopérabilité, non contraignant, fait partie de la politique d'interopérabilité de l'UE depuis 2010, dont la dernière

---

298 Règlement du Parlement européen et du Conseil, établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union (règlement pour une Europe interopérable), COM(2022) 720 final, Bruxelles, 18 novembre 2022.

299 Règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) n° 1024/2012 (OJ L 295, 21.11.2018), 2 octobre 2018.

300 Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, Bruxelles, 3 juin 2021.

301 Proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) (COM [2022] 68 finals) et la Proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données) (COM [2020] 767 finals).

302 Document de travail des services de la Commission, « résumé de l'évaluation de La DIRECTIVE 2007/2/EC établissant une infrastructure d'information spatiale dans la Communauté européenne (INSPIRE). », Bruxelles, 13 juillet 2022, p.3.

version a été adoptée en 2017[303]. L'Interoperable Europe Act vise à développer une approche cohérente de l'interopérabilité transfrontalière des réseaux et des systèmes d'information utilisés pour fournir ou gérer des services publics. Le tout accompagné d'une gouvernance claire pour rationaliser les cadres, les solutions, les lignes directrices et les spécifications d'interopérabilité partagés dans le contexte de la fourniture de services publics numériques transfrontaliers au sein de l'UE.

L'échelon européen constitue une des échelles les plus importantes pour la France concernant la normalisation et la diffusion des informations géographiques. La défense de la gouvernance française en matière de production de données géographiques, passe par son intégration au sein de l'Union européenne et de sa collaboration avec les autres pays membres de l'Union. En assurant une stratégie coordonnée de production et de normalisation des données géographiques avec la directive, INSPIRE, et ses initiatives pour promouvoir un espace commun de données, l'Union européenne sont un acteur important de la défense des intérêts français. L'espace européen offre une infrastructure sans équivalent dans le monde en matière de coopération régionale, qui n'est rendu possible que par le travail en matière de normalisation effectué par les experts de l'IGN et leurs homologues européens. Ce travail assure à la France et à ses partenaires européens, un outil puissant pour mettre en place des politiques transnationales d'aménagement du territoire, levier essentiel à la protection de la souveraineté territoriale française, mais également à la protection des environnements transfrontaliers et au développement des infrastructures transnationales. La normalisation de ces données et leur réutilisation participent également de la défense du territoire français en permettant une coopération approfondie des acteurs européens de la défense et la constitution de cartes unies à l'échelle du continent. De fait, la normalisation des données géographiques est également un enjeu de premier plan pour les militaires, qui disposent de leurs propres acteurs et organismes tournés vers la normalisation des données géographiques afin de répondre à leurs besoins.

[303] Communication de la commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions, Cadre d'interopérabilité européen – Stratégie de mise en œuvre (COM [2017] 134 finals), Bruxelles, 23 mars 2017.

3. Les acteurs de la normalisation de données géographiques militaires

3.1 Le Defence Geospatial Information Working Group (DGIWG)

Fondé en 1983, le Defence Geospatial Information Working Group (DGIWG) est un organe multinational regroupant 24 nations[304], pour la plupart membres de l'OTAN, liées par un protocole d'accord. En plus de ses membres, le DGIWG compte également quatre organisations partenaires : l'ISO/TC 211 « Geographic information/Geomatics », l'Open Geospatial Consortium (OGC), l'International Hydrographic Organization (IHO), et le Centre satellitaire de l'Union européenne (CSUE). Le DGIWG a pour but de répondre aux besoins d'échange d'information géospatiale de ses différents membres pour les exercices et opérations multinationales auxquelles ils participent. Bien qu'il ne s'agisse pas d'un organisme de l'OTAN, il répond aux exigences de l'Alliance atlantique et des autres alliances auxquelles participent ses pays membres, y compris les opérations de maintien de la paix sanctionnées par l'ONU. Le DGIWG définit des composantes d'information à utiliser dans l'élaboration de spécifications de produits et de schémas d'application pour les données géospatiales militaires. Le DGIWG établit également des spécifications de services, des formats d'encodage et des méthodologies de test pour répondre aux exigences du renseignement géospatial militaire. Le DGIWG met l'accent sur le développement de normes ouvertes afin de fournir des modèles de données capables de s'adapter aux besoins opérationnels de ses membres, tout en maintenant un maximum de flexibilité dans la conception de ces normes.

Le DGIWG cherche à répondre aux défis de l'interopérabilité au sein d'opération en coalition en créant les normes, les orientations de mise en œuvre et les procédures nécessaires pour permettre la fourniture, l'échange et l'utilisation d'informations géospatiales normalisées. Le DGIWG a développé la suite de normes DIGEST (Digital Geographic Information Exchange Standard), y compris le Feature and Attribute Coding Catalogue (FACC) et le DGIWG Feature Data Dictionary (DFDD), sur lesquels sont fondées les spécifications actuelles et futures des produits et des données militaires[305]. Bon nombre des normes élaborées par le DGIWG reposent sur les normes génériques et abstraites relatives aux informations géographiques définies par l'Organisation internationale de normalisation (ISO/TC 211). À titre d'exemple, on peut citer la série de normes ISO/19159 portant sur la calibration et la validation

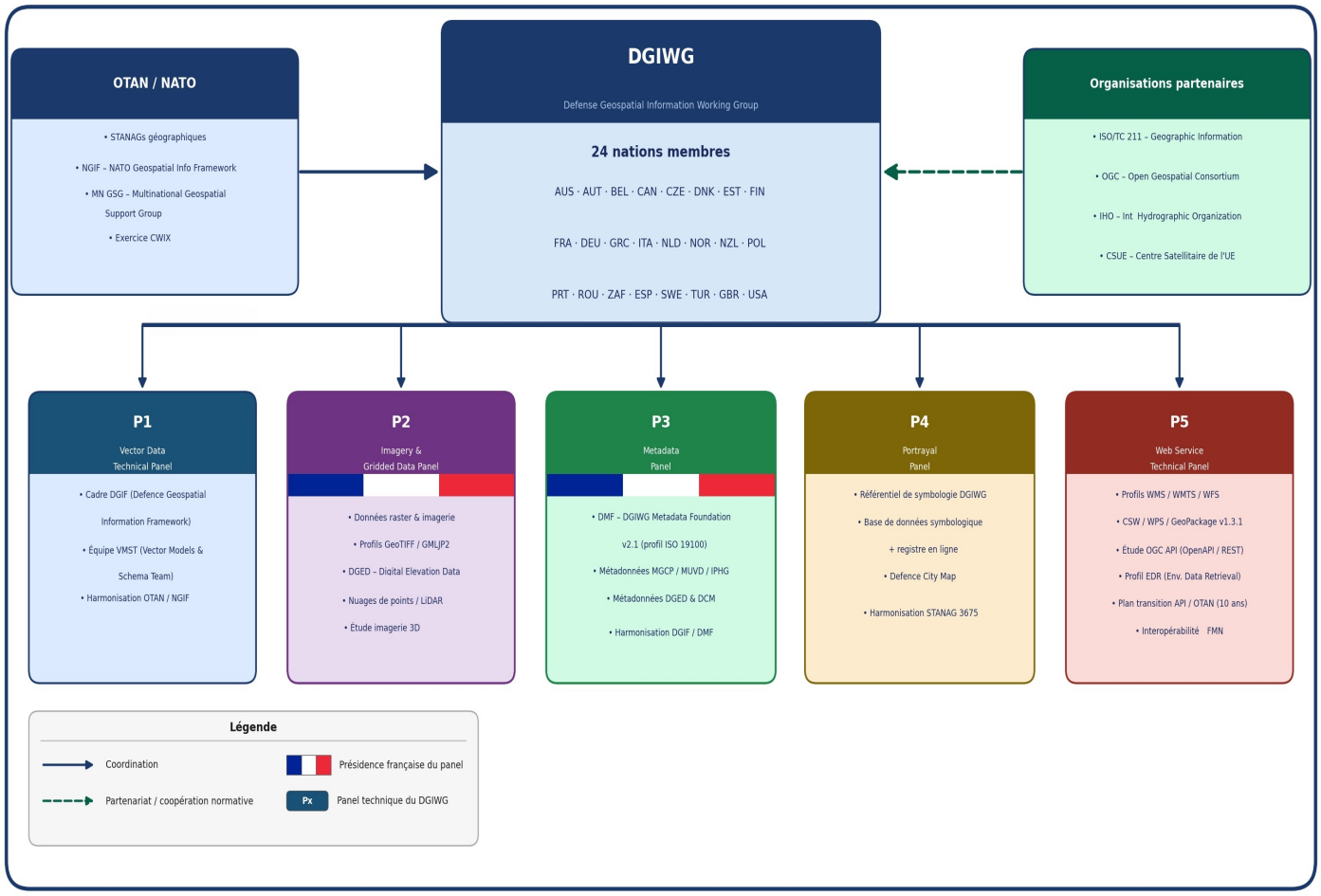
[304] Site officiel du DGIWG : https://dgiwg.org/membership/

[305] Geospatial Intelligence Standards Working Group, « Geospatial Intelligence standard : Part 2 : Overview of GEOINT Standards », On-line training modules sponsored by the Geospatial Intelligence Standards Working Group (GWG), 30 janvier 2007.

de capteurs de télédétection développées par l'ISO/TC 211 qui sert de support au développement des normes du DGIWG en matière de télédétection. Le DGIWG utilise également les normes de services Web développées par L'Open Geospatial Consortium (OGC) Le DGIWG maintient également des liens avec l'Organisation internationale d'hydrographie (International Hydrographic Organization : IHO), ainsi qu'avec le centre satellitaire européen. Ainsi, l'ensemble des organisations de normalisation cherchant à répondre aux défis de l'interopérabilité du milieu militaire sont intimement liées, assurant une coordination optimale entre les différents participants. De plus, les individus en charge de la normalisation des données géographiques militaires comme civils sont souvent les mêmes, du fait du nombre relativement restreint de personnes engagées dans ces activités. De ce fait, l'articulation entre les différents groupes de travail de ces organisations est garantie également par une forte endogamie de leurs membres, renforçant la coordination des différents acteurs impliqués dans ces mécanismes de normalisation. Comme indiqué précédemment, la France joue un rôle historique de premier plan dans les processus de normalisation des données géographiques civils. Sa présence au sein d'organismes comme l'OTAN et le DGIWG lui permet également de peser dans les décisions prises en matière de normalisation militaire et d'assurer une cohérence dans le développement de normes internationales dans ces deux domaines.

Le DGIWG compte aujourd'hui 33 standards actifs. Les standards du DGIWG sont d'une importance particulière, en ce qu'ils fournissent les fondations de la majorité des standards adoptés par les forces armées françaises, en matière de production et d'exploitation de données géographiques. De plus, la majorité des standards de l'OTAN (STANAGs) en matière d'information géographique sont souvent conçus en collaboration avec le DGIWG.

Figure 9 : Structure du Defence Geospatial Information Working Group (DGIWG)



Source : *Recherche de terrain de l'auteur (2022-2024) et DGIWG*

Le DGIWG est organisé en cinq groupes de travail, appelés panels techniques, couvrant l'ensemble des besoins en matière de production de normes géographiques pour les armées. Le panel numéro 1 (P1) est appelé panel technique sur les données vecteurs ou Vector Data Technical Panel et se concentre sur le développement et la mise à jour des normes et des spécifications permettant l'échange efficace d'informations et de produits géospatiaux vectoriels. Le P1 est en charge du maintien du Cadre d'information géospatiale de défense (Defence Geospatial Information Framework [DGIF]). Le DGIF est un ensemble de spécifications englobant différents types d'informations géospatiales, météorologiques, océanographiques et aéronautiques. Le DGIF fournit un modèle commun permettant un échange d'informations standardisé et la création de produits géospatiaux standardisés. Ces normes ont pour but de créer des passerelles d'interopérabilité entre les schémas de données des différents pays concernés, afin de permettre la création de produits géospatiaux et de services de données cohérents

pour l'utilisateur final. Au sein du P1, l'équipe en charge des modèles et des schémas vectoriels (Vector Models and Schema Team (VMST)) est l'équipe permanente responsable de la maintenance et de l'évolution du DGIF et de ses composants. L'équipe VMST est également en charge d'harmoniser les modèles et schémas vectoriels pour le domaine maritime, en s'appuyant sur la norme S-100 de l'IHO, ainsi que les modèles de données de l'OTAN. Elle est également en charge de répondre aux besoins des programmes de coproduction, tels que MGCP auxquels participent la majorité des membres du DGIWG, ainsi que ceux du programme IPHG en matière de données de géographie humaine. Les besoins de l'OTAN sont au cœur du travail du P1, et l'harmonisation entre le DGIF et le NGIF (NATO Geographic Information Framework) constitue une tâche permanente pour le P1. L'extrême interconnexion entre les différents acteurs, à la fois de l'OTAN, des programmes de coproduction géographiques militaires et des membres du DGIWG est bien reflétée par le travail du P1 et des autres panels. Ainsi, le DGIWG joue un rôle actif dans le soutien non seulement à l'OTAN, en permettant la création de passerelles entre les normes OTAN et le reste du monde de la défense, mais également aux programmes de coproduction qui s'appuient sur des spécifications, qui ne sont pas des standards. La production de standards en matière d'échange de données vecteurs pour les programmes de coproduction doit permettre à terme de fluidifier les échanges de données au sein de ces programmes, tout en allégeant la charge de travail de ces groupes de coproduction, qui n'ont ni le temps ni le personnel pour s'adonner à la création de norme en plus de leur production de données.

Le P2 s'intitule panel imagerie et données maillées (Imagery and Gridded Data Panel). Il est en charge de développer ou de recommander des normes relatives aux données raster (imagerie, cartes, élévation). Six normes ont été développées par le P2. Deux profils d'application concernant l'emploi du format GeoTIFF et GMLJP2. Une spécification concernant les données d'élévation de surface (modèle, schémas et encodage), ainsi que trois profilés d'implémentations, pour les données d'élévation (DGED), les cartes (DRP) et les orthoimages (DOP). Les travaux du P2 sont tournés vers l'innovation en matière de données images, notamment concernant l'emploi de la 3D par les forces armées, avec à la clé un possible standard en matière d'imagerie 3D. Les nuages de points[306] sont ainsi étudiés par le P2, comme le modèle JPEG Pleno, une nouvelle variante du format JPEG qui vise à fournir un modèle normalisé pour représenter les nouvelles modalités d'imagerie, tels les nuages de points. Le modèle LAS[307], déjà adopté comme une norme de facto par certains acteurs, notamment à l'OGC où il a été

[306] Un nuage de points fait référence à des données représentant les positions de points dans l'espace, exprimées dans un système de coordonnées tridimensionnelles que l'on appelle géométrie. Ces données géométriques peuvent être accompagnées d'attributs par point de différente nature (par exemple, la couleur). Ces ensembles de données sont généralement acquis à l'aide d'un scanner 3D, de la technologie LIDAR ou créés à l'aide d'un logiciel de conception 3D et peuvent ensuite être utilisés pour représenter et restituer des surfaces 3D. Les nuages de points ouvrent un large éventail de possibilités, notamment pour les applications de navigation immersive et de réalité virtuelle.

[307] Le format LAS (LASer file format) est un format de fichier conçu pour l'échange et l'archivage de données de nuages de points lidars. Il s'agit d'un format binaire ouvert créé par l'American Society for Photogrammetry and Remote

désigné comme norme communautaire, est également étudié, aux côtés d'autres normes, telles que HDF5[308], ou encore SIPC (Sensor Independent point cloud) développé par la NGA américaine. La conception d'une norme DGIWG, développée spécialement pour répondre aux besoins des acteurs de la défense, est en cours d'étude. La normalisation de tels formats de données de nuages de points permettrait de faciliter les échanges de modèles numériques de terrains obtenus en opération entre différents membres de la coalition. Un livre blanc concernant l'usage des nuages de point pour les forces armées a été publié sur le site du DGIWG le 24 octobre 2023, afin de présenter les besoins potentiels des acteurs de la défense en matière de normalisation concernant le traitement des données issues de nuages de points à différents stades du cycle de vie des données : acquisition, modélisation, encodage, diffusion et description. Il est également à noter que le P2 fait partie, avec le P3, des deux panels du DGIWG présidés par des représentants français, signe de la forte implication de la France dans cet écosystème normatif, et de la reconnaissance du savoir-faire des experts français de l'IGN en la matière.

Le P3 est le panel Métadonnées. Les métadonnées sont essentielles pour traiter les données géospatiales. Sur les cartes imprimées, l'utilisateur peut trouver des informations sur le contenu, la spécification du produit, l'actualité des sources de données, le producteur, le distributeur, l'échelle et d'autres données importantes pour l'utilisation de la carte. Pour les données géospatiales numériques, ces métadonnées doivent être fournies en plus des données proprement dites. Les métadonnées numériques doivent être structurées, c'est-à-dire que les éléments de métadonnées, leurs types de valeurs, leurs obligations et la multiplicité de leurs occurrences doivent être définis. Chaque infrastructure de données spatiales reste spécifique en termes d'utilisateurs, d'exigences, de pratiques, de cultures et de politiques. Ainsi, l'adoption de normes en matière de métadonnées devient essentielle lorsqu'il s'agit de mettre en relation différentes infrastructures de données spatiales. Les acteurs de la défense ont depuis longtemps adopté les normes de métadonnées civiles (ISO 19115, ISO/TS 19139, etc.). Dans le but de disposer d'un profil normalisé de métadonnées pour la communauté militaire, le P3 a créé le DMF (DGIWG Metadata Foundation), un profil général de métadonnées pour les jeux de données, les séries, les services, les tuiles, les documents, les produits et les données non géographiques, fondés sur les normes de métadonnées ISO de la série de normes ISO 19100. Le DMF en est aujourd'hui à sa version 2.1 et continue d'harmoniser les métadonnées d'un nombre toujours plus important de jeux de données issues de producteurs différents. Le DMF est en constante évolution, du fait de l'évolution des besoins des acteurs de la défense en matière de données, ainsi qu'à cause des

Sensing (ASPRS). Ce format est largement utilisé et considéré comme une norme industrielle pour les données lidars.

[308] Le format de données hiérarchiques (HDF) est un ensemble de formats de fichiers (HDF4, HDF5) conçus pour stocker et organiser de grandes quantités de données. Il est actuellement étudié comme un potentiel format d'échange de données de type nuage de points.

évolutions que subissent les normes déjà établies, qui entraîne le besoin d'harmoniser le DMF avec ces nouveaux besoins. Ainsi, les changements apportés à la norme ISO 19157-1[309] publiée en avril 2023, portant sur la description de la qualité d'une donnée au sein d'un jeu de métadonnée, se répercutent sur le DMF qui doit s'aligner sur ces dernières modifications. Le DMF doit également s'aligner avec le DGIF afin de faciliter la recherche et l'échange de données au sein de ce dernier. Le DMF prend également en compte les besoins du DGED, et des programmes de coproduction, tels que MGCP, MUVD et IPHG, il inclut également les métadonnées des données de type JOG-A[310], DOP pour les orthoimages, et DCM pour les nuages de points. Le DMF est donc un chantier en constante évolution, qui s'améliore à chacune de ses itérations afin de constituer un référentiel toujours plus complet de métadonnées pour les acteurs militaires. Toujours dans une logique de coopération avec l'OTAN, le panel métadonnée du DGIWG se penche sur l'intégration des métadonnées des membres de l'Alliance durant l'exercice annuel d'interopérabilité CWIX. La France a ainsi conçu un catalogue de métadonnée en demandant à l'ensemble des membres participants de fournir des métadonnées conformes au DMF provenant de leurs jeux de données nationales lors du prochain exercice CIWIX prévu en 2024, afin de mieux appréhender les besoins de l'OTAN en matière d'interopérabilité en matière de métadonnées des données géographiques.

Le panel technique n°4 se concentre sur la symbologie (Portrayal). Le principal travail du P4 consiste à maintenir un ensemble de symbologies adapté à la production de cartes numériques et papiers afin d'harmoniser les symbologies nationales des membres du DGIWG en un ensemble cohérent de symboles, adapté aux différents produits cartographiques. Un des grands chantiers du P4 est la création d'un référentiel de symbologie afin de permettre au DGIWG de stocker et gérer l'ensemble des symbologies utilisées par les nations membres du DGIWG dans un référentiel commun. Ce référentiel de symbologie se compose de deux éléments, tout d'abord une base de données symbologique, disponible sous Microsoft Access et contenant des informations concernant la façon dont les symboles ont été créés grâce à une bibliothèque de conception de symboles, ainsi que des informations à propose de la façon dont les symboles sont utilisés, grâce à des liens reliant chaque symbole à l'objet représenté sur le produit final. Enfin, un registre de symboles sera mis à terme à disposition sur Internet contenant l'ensemble des produits approuvés et ceux en cours de développement afin que les acteurs de la défense puissent suivre l'évolution des travaux du P4 en termes de symbologie. Le P4 a donc pour tâche d'harmoniser la production de symboles répondant à différents besoins, notamment ceux des programmes de coproduction. Ainsi, dans le but de produire un standard ouvert pour la symbologie des cartes urbaines au 5K, similaire aux cartes produites au sein du

[309] ISO 19157-1 : 2023 - Information géographique : Qualité des données -Partie 1 : Exigences générales, avril 2023.
[310] Le Joint Operation Graphic (Air)

programme MUVD, le DGIWG a créé le Defence City Map, en s'appuyant sur les spécifications créées pour le programme MUVD. La France qui avait largement participé à la création des spécifications pour le programme MUVD a insisté pour que le profilé du Defence City Map s'appuie sur ces spécifications déjà établies auparavant. Dans un souci de coordination avec l'OTAN, un besoin constant pour le DGIWG, le STANAG 3675 portant sur la symbologie des cartes terrestres, aéronautiques et des cartes navales spéciales, a été passé en revu afin d'importer certains symboles OTAN au sein du répertoire de symbologie du DGIWG. Le P4 est également responsable de la mise au point d'un profile Defence JOG(A), offrant une norme ouverte pour la symbologie des produits JOG(A).

Le P5 est le panel technique sur les services Web (Web Service Technical Panel [WSTP]) au sein du DGIWG. Il est en charge de promouvoir la découverte, la récupération, la dissémination et l'utilisation de données et de produits géospatiaux en créant et en maintenant des normes ouvertes et des profils de mise en œuvre pour les services Web géospatiaux. Le P5 s'intéresse tout particulièrement aux questions techniques liées aux services d'information géospatiaux, aux architectures de services Web et à leurs interfaces, ainsi qu'aux formats d'échange de données. Le P5 a développé plusieurs profilés d'implémentations de normes préalablement développées par l'OGC concernant diverses normes nécessaires à la dissémination d'informations géospatiales par des services Web. Ces profilés sont conçus pour répondre aux besoins des acteurs de la défense en restreignant ou étendant les mesures nécessaires pour être conforme à la norme proposée. Il s'agit du profile WMS (Web Map Service), WMTS (Web Map Tile Service), WFS (Web Feature Service), WCS (Web Coverage Service), CSW (Catalogue Service for the Web), WPS (Web Processing Services) ainsi que le GeoPackage. Le profilé d'implémentation du GeoPackage a connu une nouvelle mise à jour (version 1.3.1 Ed.1) le 22 septembre 2023. Les projets en cours de développement au sein du P5 sont multiples. Le nouveau profil GeoPackage est déjà en cours de révision, notamment afin de prendre en compte les nouvelles demandes exprimées par l'OTAN concernant les capacités du format GeoPackage. Le profil WPS est également en cours de révision à la suite de de nouvelles demandes de l'OTAN, et sa mise à jour est prévue pour avril 2024. Deux projets novateurs animent également les membres du P5, à commencer par l'implémentation des nouvelles API (Interface de programmation d'application ou API en anglais) développées par l'OGC afin de savoir si le domaine militaire pourrait trouver un intérêt à les implémenter. En effet, le monde des technologies de l'information a connu de nombreux changements en matière d'architecture Web pour transmettre des informations via Internet. Les architectures fondées sur les IPA sont devenues de plus en plus prévalentes ces dernières années. Ce changement d'architecture a également été adopté par l'Open Geospatial Consortium (OGC), qui définit actuellement des normes en matière d'IPA pour les opérations de ses normes de services Web (WMS,

WFS, WCS, WPS, etc.) afin de tirer parti des pratiques modernes de développement Web. L'OGC s'appuie en particulier sur la méthode OpenAPI[311] afin de développer ses normes sur un format ouvert. Les nouvelles API de l'OGC promettent de fournir des mécanismes supplémentaires d'accès aux données géospatiales à l'avenir et seront très probablement utilisées et mises en œuvre par un large éventail de développeurs et de fournisseurs. Cela a poussé le P5 du DGIWG à rédiger un premier livre blanc le 20 octobre 2023 afin d'étudier la possibilité de développer des profilés d'implémentation d'API pour la communauté militaire.

Un des défis de l'adoption d'API au sein de la communauté militaire, tient aux conséquences que cela aura sur les systèmes mis en place par l'OTAN, en particulier le Federated Mission Network (FMN) qui repose encore sur les anciens standards en matière de services Web. Faire évoluer ces standards peut prendre beaucoup de temps au sein des institutions militaires qui ont en charge de nombreux systèmes d'armes souvent anciens qui ne sont pas nécessairement capables de faire la transition vers les nouveaux modes de production d'architecture Web, comme les API. Ce défi est renforcé dans le cas d'une coalition comme l'OTAN où la moindre décision en la matière nécessite l'accord de l'ensemble des pays membres. Il n'empêche que le changement vers les nouvelles API devra se faire, et un plan de transition pour les dix prochaines années est en cours de préparation au sein du DGIWG afin d'inciter l'OTAN à préparer son propre plan de transition en vue de l'adoption de nouvelles normes en matière de service Web. Cette situation illustre bien un des nombreux défis de la normalisation qui tient à la rapidité des évolutions technologiques, qui incitent à la conception de nouvelles normes, en particulier au sein des consortiums privés, comme l'OGC, souvent en contradiction avec les rythmes beaucoup plus lents des organismes qui les implémentent. Ces derniers risquent même de voir d'un mauvais œil le développement trop rapide de normes, qui rentre en contradiction avec un des objectifs mêmes du développement de norme de leur point de vue, qui est la recherche de la stabilité au sein d'une chaîne de production. Développer une approche plus agile en matière de développement au sein des institutions militaires est un défi rencontré par tous les pays, et auquel aucune solution parfaite n'a été trouvée jusqu'à présent. Une réalité qui retarde l'adoption de normes novatrice au sein de la communauté de la défense.

Un autre projet en cours au sein du P5 est celui du profilé d'implémentation pour une IPA d'Extraction de données environnementales (Environnementale Data Retrieval [EDR]), présenté par le représentant britannique au sein du P5. Les objectifs de l'API EDR sont de faciliter l'accès à un large éventail de données par le biais d'une interface Web simple, uniforme et bien définie, et de réduire les

[311] La spécification OpenAPI (OAS) (précédemment connue sous le nom de Swagger) définit une interface normalisée et indépendante des langages de programmation pour les API, qui permet aux humains et aux ordinateurs de découvrir et de comprendre les capacités d'un service Web sans avoir à accéder au code source, à la documentation ou à l'inspection du trafic réseau.

données à celles dont l'utilisateur ou le client a besoin, tout en masquant une grande partie de la complexité du stockage des données à l'utilisateur final. L'un des principaux cas d'utilisation de l'API EDR est l'extraction de petits sous-ensembles de grandes collections de données environnementales, telles que des prévisions météorologiques. L'implémentation d'un profile EDR pourrait répondre à de nombreux besoins exprimés par les forces armées, tels que connaître les conditions météorologiques quotidiennes sur un aéroport afin de renseigner les pilotes atterrissant ou s'envolant depuis cet aéroport, ou encore connaître les conditions de l'air en altitude afin d'indiquer aux pilotes si les conditions sont propices à un décollage vertical ou pour entreprendre des missions de ravitaillement en carburant. Ce profilé d'implémentation est dérivé de la norme API – EDR développé par l'OGC. Une première version du profilé a été présentée au sein du DGIWG et est toujours en cours de rédaction, la version finale de ce profil pourrait être publiée pour avril 2024.

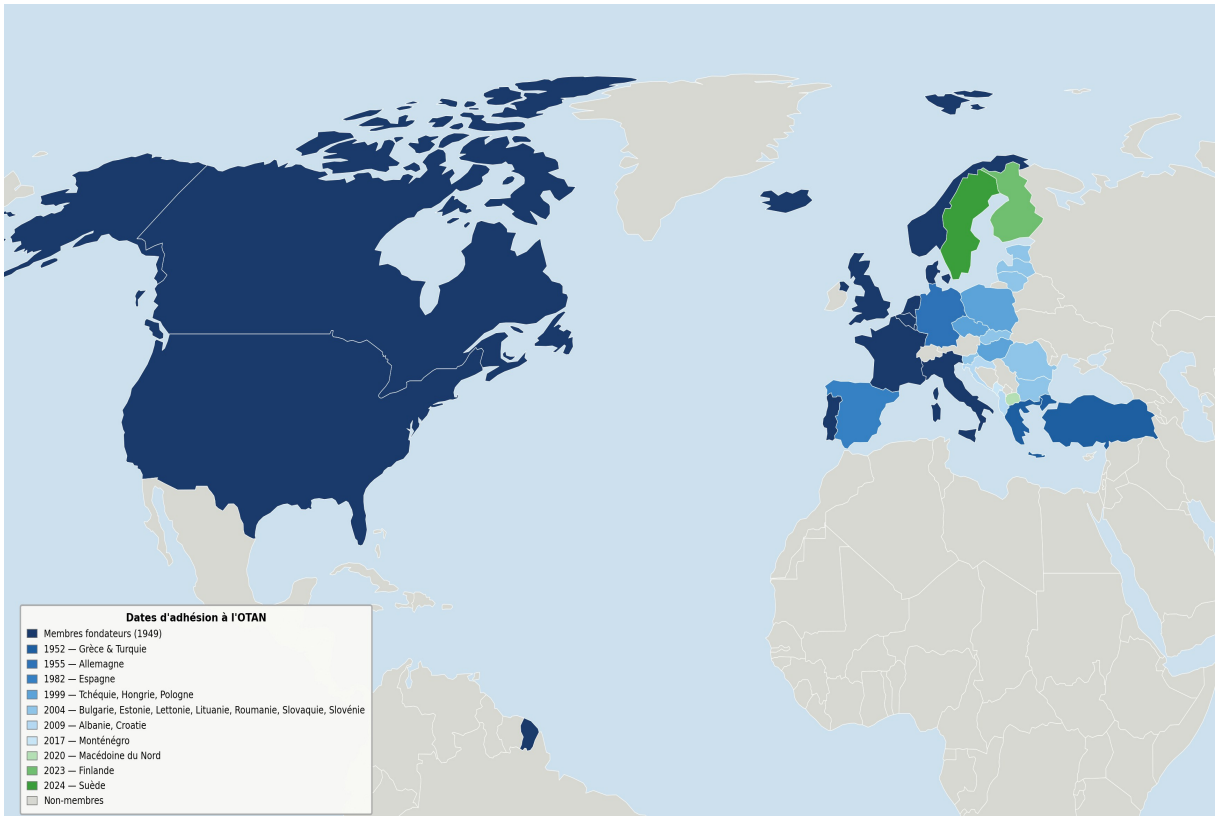
Les membres du DGIWG sont pour la plupart membres de l'OTAN, qui est également concernée par les problématiques de normalisation des données géographiques entre ces États membres. De ce fait, les deux organisations entretiennent des liens très étroits et rassemblent souvent les mêmes experts. Si l'OTAN s'appuie sur le travail mené par le DGIWG pour développer des normes, elle est également productrice de normes en interne appelées STANAG. La France, en tant que membre de ces deux organisations, s'implique à la fois au DGIWG et à l'OTAN pour représenter les besoins de ses forces armées et s'assurer que les normes employées en sein des forces armées françaises sont en cohérence avec celles développées en interne.

3.2 l'OTAN, acteur clé de la normalisation militaire occidentale

La normalisation est un débat de longue date au sein de l'Alliance atlantique, qui n'a de cesse de chercher à rendre interopérables les différents équipements employés par l'ensemble de ses membres (cf. carte 4). De par l'extrême diversité de ses membres, et de leurs différentes industries de défense, une normalisation totale des équipements de l'OTAN est impossible, en plus de ne pas être souhaitable pour de nombreuses raisons[312]. Ainsi, dans la majorité des cas, l'OTAN cherche avant tout à assurer l'interopérabilité des divers équipements employés par ses membres en se concentrant sur le plus petit dénominateur commun (par exemple, le calibre des munitions utilisées par les différents fusils en dotations au sein des membres de l'Alliance). Dans le cas des données géographiques, les besoins en matière d'interopérabilité se concentrent avant tout sur la capacité à produire des données géographiques homogènes sur l'ensemble de l'espace européen, excluant les questions d'équipement. Si exposer ainsi l'objectif peut sembler modeste, la production normalisée de données géographiques nécessite tout de même de larges efforts en matière de coopération au sein de l'Alliance, rendue difficile par la grande diversité de moyens de ses différents membres et des lacunes en matière de coopération concernant le partage d'informations géographiques. De plus, les évolutions technologiques dans le domaine de l'industrie spatiale et de l'informatique constituent des défis sans cesse renouvelés pour interopérabilité des membres de l'OTAN[313] qui sont toujours tentés de modifier leurs modes de production et de dissémination de leurs données géographiques afin d'exploiter les derniers développements en la matière, et d'appliquer les normes les plus récentes qui les accompagnent. La capacité de recueillir, de traiter et de diffuser des informations géographiques précises pour soutenir une prise de décision efficace plus rapidement que la capacité de l'ennemi à le faire a toujours été la marque de fabrique des opérations militaires efficaces. À l'heure où la plupart des systèmes sont interconnectés, avec la prolifération des capteurs et des référentiels de données, la supériorité de l'information devient rapidement un facteur décisif pour le succès de la mission. Par conséquent, la capacité des alliés à partager rapidement et en toute sécurité des informations géoréférencées aux niveaux opérationnel et stratégique, et à exploiter ces informations pour prendre des décisions communes judicieuses devient capitale.

[312] Eliot Cohen, « NATO Standardization: The Perils of Common Sense. », in *Foreign Policy*, no. 31, pp. 72 – 90, 1978.
[313] M. Hura et coll., « Interoperability: a continuing challenge in coalition operations », Santa Monica, RAND, 2000.

Carte 4 : Pays membres de l'Organisation du Traité de l'Atlantique Nord



Source : OTAN (2026)

L'OTAN a publié en 2018 le Cadre OTAN pour l'information géospatiale (NATO Geospatial Information Framework) afin de répondre au besoin de *« combattre sur la même carte »* qui avait déjà été exprimé dans la politique géospatiale de l'OTAN (MC 0296/3) en 2011[314]. Le Cadre OTAN pour l'Information géospatiale vise à mettre en place un écosystème cohérent de produits géospatiaux numériques et physiques, pour tous les domaines (terre, mer, air), du niveau stratégique au niveau tactique. Les besoins de l'OTAN en matière d'information géospatiale sont définis en fonction du type de produit (ce qui est requis, le niveau de détail à une échelle spécifique) et de la couverture (l'endroit où elle est requise)[315]. Le soutien géospatial de l'OTAN couvre l'ensemble des espaces de bataille et se compose de quatre types de produits principaux : les informations topographiques, hydrographiques et aéronautiques, ainsi que les images géoréférencées appropriées. Le soutien géospatial au sein de l'OTAN occupe une place particulière dans la chaîne de commandement. La caractéristique essentielle de chaque quartier général de l'OTAN est le multinationalisme, ce qui est autant un avantage qu'un inconvénient. Chaque service géospatial militaire national apporte sa propre expérience et ses propres

314 OTAN, « MC 0296/3 Politiques Geospatiale de l'OTAN », Bruxelles, 2011.
315 *Ibid*

traditions au service géospatial unifié de l'OTAN. L'inconvénient est qu'il est impossible de parvenir à un consensus total dans une communauté aussi diversifiée. De plus, en termes de prise de décision, il est évident que de grande disparité existe parmi les membres de l'OTAN en termes de personnel et de contribution financière, qui ont un impact direct sur la capacité des différentes nations à peser dans les décisions. À titre d'exemple, la France arrive deuxième derrière les États-Unis en termes de contribution financière et en personnels au sein de l'Alliance et cinquième pour sa contribution en ingénieurs géospatiaux (derrière les États-Unis, la République tchèque, le Royaume-Uni et l'Allemagne)[316]. Le domaine de la production de données géospatiales n'échappe donc pas à ces disparités de moyens. Si ni les effectifs exacts des ingénieurs géospatiaux ni l'étendue de la production de chaque pays ne peuvent être directement publiés, il est évident que des divergences substantielles peuvent être observées. Bien que le système de soutien géospatial de l'OTAN s'appuie sur les capacités et les moyens des États membres, il est difficile de distinguer un élément commun aux systèmes nationaux dans la hiérarchie de l'OTAN. L'institut technique géospatial le plus élevé de l'OTAN est une unité de géographes située au siège du SHAPE[317]. Elle dirige l'ensemble du système de soutien géospatial de l'OTAN d'un point de vue conceptuel. C'est également cette unité qui planifie la production, recueille des données, gère la désignation et la normalisation des produits cartographiques. Cependant, l'Alliance ne dispose pas de centre de production de donnée géographique centralisé. Les besoins en la matière sont donc couverts par les différentes capacités des États membres. En cas de crise majeure, la cellule géographique de la SHAPE dispose toutefois de fonds dont elle peut faire usage pour collecter des données ou assigner cette tâche à une agence de confiance du secteur privé.

Parmi les membres de l'Alliance, il existe un accord tacite selon lequel chaque pays de l'OTAN doit satisfaire aux exigences géospatiales minimales et cartographier au moins son propre territoire national, ses eaux territoriales et son espace aérien. Il n'est pas surprenant que cela nécessite une coordination et une coopération étroite avec les pays voisins, car les cartes des pays voisins se chevauchent, ce qui exige que les informations provenant de l'extérieur des frontières d'un pays soient opportunes, précises et homogènes. À ce titre, les États baltes sont un bon exemple de coopération et de production efficace de cartes. Ces pays étant relativement petits, la carte de vol à basse altitude (Low Flying Chart (LFC)) à l'échelle 1 : 500 000, issue de la série de cartes à petite échelle, couvre les trois États. La feuille de carte LFC a été produite conjointement par les trois États, puis imprimée par un autre membre de l'OTAN, car aucun des États baltes ne dispose de capacités d'impression à grande échelle[318]. Au sein de l'OTAN, le groupe multinational de soutien géospatial (Multinational Geospatial

316 Rada Josef, « Smart Defence : Joint geospatial support in NATO », Geoscape, vol. 13, p. 99, 5 novembre 2019.
317 Le Haut quartier Général de l'OTAN (Supreme Headquarter for Allied Powers in Europe).
318 Sprivul Andris, « Geographic support requirements for future NATO joint expeditionary missions », Kaitseväe Akadeemia, 2016.

Support Group [MN GSG]) est en charge de mener les efforts d'harmonisation en matière de production de données géospatiales des différents membres de l'Alliance. Ce groupe international opérant sous l'égide de l'OTAN a été créé en 2016, principalement dans le but d'améliorer le soutien à distance des missions de l'OTAN et de l'UE. Le GSG MN est situé à Euskirchen, en Allemagne, dans l'enceinte du centre géographique de la Bundeswehr. Le concept clé réside dans le partage collectif du personnel, de la production et des capacités matérielles des nations de l'OTAN et de l'UE. Ainsi, l'OTAN met avant tout l'accent sur la mise en place d'un environnement de coopération multinationale pour produire des informations géographiques en temps voulu propres à répondre aux besoins opérationnels. Bien que les capacités de production varient fortement d'un pays à l'autre, en fonction de leurs budgets, la coopération entre les membres de l'Alliance atlantique allège une partie du fardeau grâce au partage des connaissances et de l'expertise. Dans l'idéal, l'accord combiné de l'ensemble des pays aurait dû permettre de fournir l'ensemble des données cartographiques nécessaires pour accomplir les objectifs fixés par l'OTAN en matière de production de données géographiques. Ce n'est malheureusement pas toujours le cas, du fait d'un fossé encore trop important entre ce que peuvent fournir en temps et en heure les différentes nations. Une solution potentielle pour atteindre cet objectif consiste à partager les sources et les capacités dans le cadre de projets de coproduction, tels que le programme MGCP (Multinational Geospatial coproduction Program), et s'efforcer d'éviter ou de réduire la duplication des produits géospatiaux.

L'OTAN développe, à travers son bureau de normalisation (NATO Standardization Office (NSO)), des normes (appelées STANAGs[319]) en matière de données géographiques afin de faciliter les échanges de données et garantir une vision commune de l'environnement de déploiement pour l'ensemble des membres de l'Alliance atlantique. Il existe plus de 1 200 STANAG promulgués à l'OTAN, dont plus de 40 régulent la production de données géographiques militaires[320]. L'application de la normalisation à tous les membres de l'OTAN est une question extrêmement difficile. De nombreux problèmes persistent pour unifier les productions géographiques. L'unification des cartes topographiques à l'échelle 1 : 50 000 est un de ces problèmes. Les préparatifs en vue de la mise en œuvre de la norme sont déjà en cours, mais de nombreux pays sont encore opposés à cette idée. Certains pays, comme la République tchèque, produisent leurs cartes nationales à une échelle plus fine que le 1 : 50 000e et considérerait une normalisation de la production à cette échelle comme une régression par rapport à leur production nationale actuelle. De ce point de vue, la mise en œuvre de la norme constituerait pour eux un pas en arrière. Les cartes à plus petite échelle, par exemple, le JOG

[319] Abréviation de « Standardisation Agreement » ou accords de normalisation.
[320] Site officiel du bureau de normalisation de l'OTAN : https://nso.nato.int/nso/nsdd/main/list-promulg

250[321], sont déjà normalisées (STANAG 3600, éd. 3), de sorte que l'extension du système aux cartes à moyenne échelle semble être une étape logique, mais qui rencontre tout de même des résistances de la part de certaines nations.

Cette situation est un bon exemple du pouvoir de la normalisation, même dans un environnement militaire qui n'est pas soumis aux lois du marché. Si la normalisation a supposément pour but d'aboutir à la création du meilleur produit possible, ce n'est pas toujours le cas d'un point de vue purement technique, comme l'illustre le cas de la normalisation des cartes de l'OTAN à l'échelle 1 : 50 000e. Quand bien même certaines nations produisent des cartes plus fines, si ces dernières ne respectent pas la norme approuvée, elles seront rejetées. Ainsi, dans un « marché » où les besoins en matière d'interopérabilité priment sur d'autres considérations, comme c'est le cas à l'OTAN, la norme rend à terme obsolète même des produits pourtant plus précis. Ainsi, la maxime selon laquelle « celui qui contrôle la norme contrôle le marché » s'applique également à l'environnement militaire. À partir du moment où une norme est sélectionnée et approuvée par différentes nations amenées à coopérer, comme c'est le cas dans l'OTAN où au sein des programmes de coproduction, cette norme devient la référence par défaut qui sera attendu par l'ensemble des participants. L'omniprésence de cette donnée normalisée va finir par déformer le marché dans lequel il s'inscrit, qu'il s'agisse du « marché » fermé de l'OTAN où du marché ouvert des données géographiques civiles. Si les produits proposés ne sont pas capables de répondre aux exigences par la norme adoptée en matière d'interopérabilité, ils seront écartés sans regard pour leur qualité réelle. Ainsi, l'implication d'une nation au sein d'organismes de normalisation, notamment dans le domaine militaire, peut à terme lui faire économiser beaucoup de temps et d'argent si elle arrive à convaincre ses partenaires d'adopter une norme qu'elle maîtrise déjà où qu'elle ait participé à créer.

Les travaux du bureau de normalisation de l'OTAN sont menés en étroite collaboration avec l'Organisation internationale de normalisation, qui supervise le comité technique ISO/TC 211 Informations géographiques/géomatiques. Les normes de l'ISO/TC 211 étant développées afin de subvenir aux besoins d'un maximum d'utilisateurs et de producteurs de données géospatiales, ces normes ne répondent pas toujours aux exigences d'un environnement militaire. Afin de remédier à ces problèmes d'incompatibilité tout en appuyant ses normes sur les derniers développements en la matière sur la scène internationale, l'OTAN travaille également étroitement avec le DGIWG. Ainsi, le DGIWG entretient un contact permanent avec le Bureau géographique de l'OTAN, et élabore des normes géospatiales qui s'appuient sur les normes génériques et abstraites pour l'information géographique définies par l'Organisation internationale de normalisation (ISO/TC 211). L'implication de la France au sein de l'OTAN s'étend également à une série d'exercices en coalition nommés CIWIX servant à tester

[321] joint operation graphic 1 : 250.000

l'interopérabilité des systèmes de communications, d'information et de commandement au sein de l'Alliance atlantique. Les membres du BGHOM ainsi que ceux du bureau chargé de la normalisation de l'IGN participent conjointement à ces exercices, dans un esprit de coopération entre les différentes instances françaises de normalisation de ces données. Depuis 2021 la compatibilité du programme GEODE 4D avec les procédures et spécifications du Federated Mission Networking (FMN) de l'OTAN a pu être testée avec succès.

Si la production de cartes papier homogène reste au cœur du travail du MN GSG, l'OTAN s'est également tournée vers la création de services Web capables de distribuer des informations géographiques au sein d'une infrastructure protégée. Un service Web, le système central de services géographiques de l'OTAN (NATO Core Geographic Services System (NCGSS)), conçue avec l'aide d'Esri, est distribué via le réseau interne de l'OTAN[322]. Il s'agit d'un type normalisé de service Web géospatial où toutes les données conformes sont publiées, autrement dit les données unifiées respectant les normes de l'OTAN. Le NCGSS combine des données de base (cartes raster, imagerie satellite et aérienne, données vecteurs) et des données supplémentaires (cartes diverses, produits cartographiques spécifiques à la mission). Les ensembles de données sont organisés en trois dossiers principaux en fonction de l'échelon qu'ils représentent. Les bases de données stratégiques (Strategic Data Base [SDB]) couvrent l'ensemble du territoire de l'OTAN. Les bases de données opérationnelles (Operational Database (ODB)) ne concernent qu'une mission à l'étranger ou un commandement. Les bases de données tactiques (Tactical Database (TDB)) sont produites et administrées uniquement par une cellule géographique précise à l'échelon tactique en fonction des besoins[323]. Ces outils permettant de travailler sur la composition d'une carte font partie intégrante du NCGSS. Cela permet aux responsables SIG locaux de chaque commandement de créer sans effort leur propre carte ou jeu de données. Cependant, la cellule géographique de l'OTAN ne dispose pas de sa propre branche de R&D. Le service Web NCGSS et les autres projets de recherche affiliés sont généralement confiés à l'Agence OTAN d'information et de communication (NATO Communications and Information Agency (NCIA))[324]. La NCIA est une agence civile en charge du développement des technologies C4ISR (commandement, contrôle, communication, informatique, renseignement, surveillance et reconnaissance) pour l'OTAN. Si le NCGSS est employé par l'ensemble des membres de l'Alliance, il ne constitue pas aujourd'hui un système entièrement centralisé pour la distribution d'informations géographiques. En effet, lors d'un déploiement des forces de l'OTAN, un réseau sécurisé propre à la mission est déployé qui agrège des données locales, et qui n'est que ponctuellement mis à jour avec le

322 Teufert John F., « The NATO Core Geographic Services System : Enterprise GIS for Defense Provides Strong, Centralized Geospatial Capabilities », Esri, 2014.
323 Rada Josef, « Smart Defence : Joint geospatial support in NATO », Geoscape, vol. 13, p. 102, 5 novembre 2019.
324 Agence OTAN d'information et de communication (NCIA). https://www.nato.int/cps/fr/natohq/topics_69332.htm

NCGSS, ce qui peut entraîner des situations chaotiques lors de la recherche d'information d'un réseau à l'autre et des problèmes de communications entre les membres de la mission et leurs homologues restés en Europe. Un service Web unique et centralisé contenant l'ensemble des informations disponibles à l'OTAN, accessibles également par les militaires déployés à l'étranger, pourrait être un moyen d'éviter les éventuelles erreurs d'interprétation nées d'informations provenant de deux sources distinctes. L'implémentation d'un tel système n'est cependant pas encore d'actualité. Cela nécessiterait d'importants efforts en matière d'harmonisation entre les différents réseaux SIG nationaux de chaque nation et le NCGSS, ce qui rend cette solution difficilement applicable à l'heure actuelle.

Si l'OTAN assure le développement de normes en matière de production géographiques pour ses membres. Ces travaux ne constituent pas les seuls efforts visant à produire des données géographiques dédiés aux opérations en coalition. Dès la fin des années 90, plusieurs nations menées par les États-Unis se sont mises en tête de produire des données cartographiques à l'échelle du globe. Ces efforts ont abouti à la création des programmes de coproduction internationaux. Ces derniers ont étendu largement le parc des pays concernés par ces efforts, ne se limitant pas à l'Alliance atlantique. La France participe activement à l'ensemble de ces programmes depuis leurs créations. Ils représentent aujourd'hui des enjeux de premier plan en matière d'acquisition de données pour les armées françaises. Étant par nature internationaux, ces programmes nécessitent une étroite coopération de l'ensemble des parties prenantes et imposent un important travail de normalisation afin de produire des données interopérables sur l'ensemble des zones couvertes par les différents programmes.

3.3 Les programmes de coproduction : un outil essentiel de la production de données géographiques militaires pour l'armée française

Avec la généralisation de l'informatique parmi les armées occidentales dans la seconde moitié des années 2000, l'interopérabilité des données devient une question cruciale, en particulier pour les membres de l'Alliance atlantique. Aujourd'hui, on s'attend à ce que plus de 85 % des informations opérationnelles soient fondées sur des données de positionnement géospatial ou des informations géoréférencées[325]. Par conséquent, l'utilisation de produits normalisés est d'une importance capitale pour la compréhension de l'architecture géospatiale globale, pour le développement des connaissances opérationnelles et, surtout, pour éviter l'utilisation inappropriée des données. La nécessité d'uniformiser les données afin de les rendre utilisables par l'ensemble des acteurs, qu'il s'agisse du géoréférencement, des formats ou des bases de données, va conduire les membres de l'OTAN à développer les premiers programmes de coproduction militaire de données géographiques.

Lancé en 2003 afin de remplacer le Vector Map Level 1 Coproduction Working Group (VaCWG) créé en 1994[326], le Multinational Geospatial Coproduction Project (MGCP) est le plus ancien de ces programmes encore en activité. Lancé sous l'égide de la National Geospatial-Intelligence Agency (NGA), le programme MGCP comptait à sa création en 2003, 28 membres, dont la France. Aujourd'hui (2023) le programme MGCP compte 30 membres actifs[327]. Liées par un protocole d'accord, les nations membres du programme MGCP ont pour objectif de produire une base de données géographiques numériques centralisée, composés de données vecteurs haute résolution (High Resolution Vector data : HRVD) aux échelles 50 000e et 100 000e de la Terre. À l'origine, les membres du programme MGCP ont découpé la Terre en 3200 degrés carrés répartis sur l'ensemble des terres émergées de la planète et distribué la production de ces degrés carrés entre les différents membres du programme, proportionnellement à leurs capacités de production. Afin de garantir la parfaite interopérabilité entre les jeux de données produits, la saisie de l'ensemble des objets présents sur les produits finaux est régie par un document technique de référence (Technical Reference Document [TRD]) régulièrement mis à jour au gré des demandes de changement et d'amélioration qui accompagnent l'évolution du programme. Ce dernier présente les règles de packaging, les règles d'emploi du format shapefile, les règles de saisie des objets, le catalogue des objets possibles et leurs

---

325 Crook Anthony, « Allied Command Operation Geospatial Handbook. », OTAN, Naples, 30 juillet 2009.

326 Philippe Boulanger, « La géographie reine des batailles », Perrin, 2020.

327 Les 32 membres du programme MGCP sont les suivants : Australie, Belgique, Canada, Croatie, Tchéquie, Danemark, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Italie, Japon, Corée, Lettonie, Lituanie, Moldavie, Pays-Bas, Norvège, Nouvelle-Zélande, Pologne, Portugal, Roumanie, Slovaquie, Espagne, Suède, Turquie, Royaume-Uni et États-Unis.

attributs, les spécifications des métadonnées à employer et les informations sémantiques à respecter. Il en est aujourd'hui à sa cinquième itération.

La France s'est vu attribuer au début du programme 52 degrés carrés. La première phase du programme MGCP s'est étendue de 2007 à 2011 et ce dernier a été un succès retentissant, garantissant la poursuite de la production de données MGCP jusqu'à aujourd'hui. Entre-temps les degrés carrés couverts par le projet ont progressivement augmenté, après que ce dernier ait été renouvelé jusqu'en 2025. Ainsi, en 2023, les membres du programme MGCP ont complété 5336 degrés carrés couvrant la quasi-totalité de la planète, dont 856 ont déjà fait l'objet d'une actualisation[328]. L'ensemble des données produites sont stockées au sein de l'entrepôt géospatial international (International Geospatial Warehouse : IGW) développé par la NGA. L'IGW se présente sous la forme d'un géoportail en ligne uniquement accessible aux membres du programme, où ces derniers peuvent consulter en temps réel les produits en cours de préparation par les autres pays et télécharger les données auxquels ils ont droit. En effet, le découpage de la planète en degré-carré ne sert pas uniquement à la répartition du travail entre les différents membres.

Un système de quota a ainsi été mis en place pour déterminer la quantité de données accessible à un membre du programme relativement à sa contribution. Une façon de pousser les membres du programme à accroître leur contribution afin de pouvoir en retirer un plus grand bénéfice en termes d'accès aux données. Ce système de quota sert également à attirer d'autres nations à rejoindre le programme, puisque la production du moindre degré carré de donnée permet d'accéder immédiatement à deux degrés carrés déjà produits. Le ratio de données produites/offertes ce présente de la façon suivante : Pour une à dix cellules de données, le ratio de retour est de deux pour un (par exemple, le participant reçoit deux cellules pour chaque cellule déposée jusqu'à dix cellules). De 11 à 50 cellules de données, le ratio de retour passe à quatre pour un. De 51 à 150 cellules de données, le ratio de retour est de six pour un. Pour 150 cellules ou plus, le ratio de retour est de huit pour un. Enfin, une fois atteinte la somme de 200 cellules livrées, une nation peut demander à acquérir le statut de Nation Majeur (ou *Lead Nation*), qui lui octroie un accès à l'ensemble des données produites au sein du programme. Dans ce programme, la France a démontré sa très grande implication et son excellente capacité de production en livrant 68 degrés carrés et en en actualisant 154 pour un total 839 à la date d'avril 2023[329]. Ce chiffre impressionnant de production la place en première position en termes de production de données au sein du programme MGCP, devant les Américains qui en ont produit 642 et actualisé 42 pour un total de 690.

[328] « MGCP cochair/PG Program Report », Plenary Group meeting 41, Strasbourg, 26 avril 2023.
[329] « MGCP PG41 French Report », Plenary Group meeting 41, Strasbourg, 26 avril 2023.

Les nations membres du programme MGCP sont divisées entre nations partenaires et nations majeures en fonction de leur implication. Pour obtenir le statut de nation majeure, il ne suffit pas de cumuler 20 degrés carrés produits hors de son territoire national comme signalé précédemment. Il est également nécessaire de s'impliquer dans le processus de contrôle qualité par lequel passe l'ensemble des données produites, en prenant en charge le contrôle des données produites par d'autres nations. La France a fait partie des Premières Nations à atteindre le statut de lead nation, dès 2008 (il est à noter que les États-Unis et l'Allemagne ont obtenu immédiatement le statut de Lead Nation, en prenant en charge l'ensemble du contrôle qualité des données produites durant la première année du programme, ce sont également elles qui contrôlent les données produites par les nations non « Lead Nations »). Le programme MGCP compte aujourd'hui 12 Lead Nations que sont la France, les États-Unis, le Royaume-Uni, l'Allemagne, la Norvège, le Danemark, la Suède, l'Espagne, l'Italie, l'Australie, le Canada et la Finlande, qui ont officiellement accédé à ce statut en avril 2023 après quinze ans d'activités au sein du programme.

Le programme MGCP rassemble donc un ensemble de pays hétéroclites aux capacités de production qui le sont tout autant. Si cela n'a pas empêché la réussite du programme, qui se poursuit toujours aujourd'hui, la question de la répartition équitable de la charge de travail se pose néanmoins au vu de ces disparités. MGCP repose sur des normes préétablies pour ses formats de données et d'échange, en se fondant notamment sur les profils édités par le DGIWG. Ainsi, les métadonnées du programme MGCP respectent le profilé DIGEST conçu par le DGIWG et dérivé des normes ISO 19115 et ISO 19139 concernant l'encodage des métadonnées.

Suite au succès du projet MGCP, l'idée d'étendre les programmes de coproduction à d'autres données a fini par émerger. Le premier de ces nouveaux projets a été le programme MUVD (Multinational Geospatial Co-Production Program Urban Vector Data). Lancé en 2018, le programme MUVD est directement dérivé du programme MGCP et a pour but de produire des données vecteurs hautes résolutions à l'échelle 5 000e sur des zones urbaines. Il compte aujourd'hui (2023) dix-sept participants, dont la France, le Japon est le dernier pays à avoir rejoint le programme, en octobre 2023[330]. Contrairement au programme MGCP, le but du programme MUVD n'est pas de couvrir l'ensemble des villes de la planète, les villes choisies sont à la discrétion des membres participants au programme, qui choisissent leurs zones d'intérêts en fonction de leurs intérêts nationaux. Le tout, en respectant autant que possible la stratégie globale du programme, qui consiste à produire avant tout des données sur des zones présentant un intérêt du point de vue sécuritaire, tout en cherchant à éviter la

[330] Les nations membres de MUVD sont les suivantes : Australie, Belgique, Brésil, Canada, Espagne, Estonie, Finlande, France, Royaume-Uni, Hongrie, Lituanie, Pays-Bas, Norvège, Suède, Turquie, Japon, États-Unis.

duplication des efforts[331]. Tout comme le programme MGCP, MUVD conserve le système d'acquisition de crédits afin de classer le niveau d'implication des différentes nations membres. Afin de pouvoir accéder au catalogue de données créées par l'ensemble des participants, une nation doit produire au minimum 100 crédits de données chaque année. Si une nation produit plus de 100 crédits en une année, tous les crédits supplémentaires sont comptabilisés pour l'année suivante, et ce, jusqu'à 300 crédits supplémentaires. Autrement dit, si une nation produit 400 crédits en une année (le maximum cumulable), elle n'aura pas à produire d'autres projets pendant les trois prochaines années, tout en ayant accès à l'ensemble des données produites au sein du programme. Si le système de crédits est conservé, ce n'est pas le cas du découpage en degré carré, qui ne sied pas à la délimitation des zones urbaines produites dans le programme MUVD. Pour MUVD, la zone d'intérêt peut être délimitée par n'importe quelle forme géométrique, y compris un polygone. Le processus de calcul des crédits consiste d'abord à classer la surface de la Terre en cinq catégories. Un coefficient de complexité est attribué à chaque catégorie. Pour calculer la valeur du crédit, ce coefficient est multiplié par la surface en kilomètres carrés. Les catégories sont définies de la façon suivante (cf. Tableau 4) :

Tableau 4 : Matrice de calcul des crédits MUVD

Catégorie	Description	Coefficient
Basique	Zones homogènes, avec une faible variabilité des caractéristiques et des attributs, en particulier pour la couverture du sol (surfaces naturelles : sols tels que les dunes ou la végétation clairsemée, surfaces et rivières…).	0.8
Rural	Zone plus complexe que la zone basique. Zone qui présente une grande variété de caractéristiques et d'attributs naturels (végétation : formations arborées, arbustes, herbacés…) ou des traces de présence humaine	1.2

[331] « MGCP Urban vector Data Annex C », V.1.3, 19 août 2019.

	(parcelles, habitations).	
Périphérique	Zone caractérisée par un habitat clairsemé, zone caractérisée par des zones de production et de services (production primaire, secondaire ou tertiaire, transport et infrastructure), ainsi que certaines zones anthropisées (telles que les routes, les places, les parkings, les zones d'excavation, les installations sportives ou récréatives…).	1.8
Dense	Zones caractérisées par la prépondérance d'un habitat dense (espace structuré par des bâtiments et des routes : routes, chemins).	2.6
Forte	Zones caractérisées par la prépondérance d'un habitat très dense.	3.6

Source : *Recherche de l'auteur*

Le crédit est calculé en multipliant la superficie en kilomètres carrés de chaque classe par son coefficient.

Le programme MUVD partage également avec son prédécesseur la création d'un document technique de référence (Urban Technical Reference Document (UTRD)), lui-même directement issu de celui créé pour MGCP, mais adapté à la saisie d'objets à l'échelle 5 000e. L'UTRD a connu deux versions jusqu'à aujourd'hui et continue d'être modifié, comme le TRD au fil du développement du programme. L'existence de ces deux documents de références intimement liés souligne bien le souci d'interopérabilité qui anime l'ensemble des acteurs de ces programmes de coproductions. Chaque programme s'inscrivant ainsi dans un écosystème d'informations géographiques interopérables destiné à soutenir les opérations en coalition. Non seulement le programme MUVD s'appuie-t-il sur les expériences acquises précédemment durant la production des données MGCP, mais, tout comme son ancêtre, le modèle de donnée de MUVD est développé en étroite collaboration avec le DGIWG qui

travaille en parallèle à la création d'une norme pour les données urbaines dédiées à la défense intitulée « Defense City Map ». Une première ébauche de projet a été déposée par le DGIWG le 4 juillet 2022, fruit de la collaboration des groupes dédiés à la symbologie et aux vecteurs au sein du DGIWG. Sous réserve de validation, la version finale de cette norme devrait être publiée en mai 2024.

Lancé en 2016, le programme TREx est un programme de coproduction multinational durant lequel les données collectées par les satellites de la mission TanDEM-X sont acquises, traitées, éditées et stockées dans un référentiel central [332]. Le programme TREx est aujourd'hui (2023) composé de 33 nations, dont la France[333]. La mission TanDEM-X a été mise en place sous la forme d'un partenariat public-privé, DLR[334] représentant le côté public et Airbus Defense & Space Geo GmbH (ADS) le côté privé [335]. Le programme d'échange de données d'élévation à haute résolution TanDEM-X (TREx) est basé sur le système radar satellitaire TanDEM-X capturant des données dans une résolution de 12 mètres sur l'ensemble de la planète. Tout comme le projet MUVD, les principes fondateurs de la coopération internationale pour le projet TREx sont calqués sur ceux du projet MGCP. Les nations participantes peuvent récupérer une partie proportionnelle au crédit accumulé en traitant les données qui leur sont attribuées. Le jeu de données d'élévation global créé par la mission TanDEM-X est d'une grande valeur pour la communauté scientifique et trouve des applications dans les domaines de la défense, des secours en cas de catastrophe, ou encore de la gestion du territoire. La donnée brute produite par les satellites est le résultat d'une chaîne de traitement entièrement automatisée, et contient encore des effets indésirables causés par la technologie d'acquisition SAR interférométrique, en particulier dans les régions de terrain escarpé et au-dessus de l'eau. L'objectif principal du programme TREx est l'élimination de ces effets et la fourniture d'un modèle numérique d'élévation global et homogène de la masse terrestre, le tout en moins de dix ans. Ainsi, le programme TREx doit s'achever au plus tard en décembre 2026, avec plusieurs nations ayant déjà rempli leurs objectifs de production quitteront le programme avant cette date. La France en fait partie, et a déjà annoncé son retrait du projet TREx pour 2024.

Les opérations militaires menées depuis le début de la guerre froide, à commencer par les guerres de décolonisations, en passant par les conflits plus récents en Irak (2003-2011) et en Afghanistan (2001-2021) ont montré la nécessité de comprendre les divisions religieuses, linguistiques, ethniques et autres de ces pays, ainsi que la nécessité de l'expertise culturelle de la géographie humaine

---

332 « TanDEM-X High Resolution Elevation Data Exchange (TREx) READ ME For TREx DEM Finished », janvier 2018.

333 Les nations qui composent le programme TREx sont les suivantes : Allemagne, États-Unis, Danemark, France, Pologne, Italie, Israël, Canada, Pays-Bas, Norvège, Turquie, Émirats arabes unis, Australie, Espagne, Belgique, Brésil, Chili, Finlande, Grèce, Japon, Colombie, Croatie, Lettonie, Nouvelle-Zélande, Portugal, Roumanie, Suède, Slovaquie, Afrique du Sud, Corée du Sud, Tchéquie, Royaume-Uni, Mexique.

334 Deutsches Zentrum für Luft- und Raumfahrt : Le Centre allemand pour l'aéronautique et l'astronautique.

335 Airbus DS Geo GmbH, « "EULA" DEM Data Alliance Nation », 2016.

axée sur ces régions. Le développement de doctrines ayant trait à la guerre contre-insurrectionnelle a commencé au sein de l'armée française durant la guerre d'Indochine, puis d'Algérie. C'est cette doctrine militaire qui vise à obtenir le soutien de la population dans le cadre d'un conflit opposant un mouvement insurgé à une force armée gouvernementale de contre-insurrection, qui s'est penché pour la première fois dans l'histoire militaire contemporaine sur la nécessité de l'intégration du facteur humain dans les affrontements. Dès les années 1960 d'autres nations, les concepts mis en place par la doctrine militaire de contre-insurrection se diffusent au sein d'autres pays, comme le Brésil, où le lieutenant-colonel Carlos de Meira Mattos reprend ce concept après le coup d'État militaire de 1964 dans sa lutte contre les forces anti-putschistes[336]. Cette doctrine trouve également sa place aux États-Unis à la suite de la diffusion des écrits des officiers français David Galula[337] dans les années 1960 et dont les théories influenceront l'état-major américain durant la guerre du Viêt Nam et plus tard en Irak et en Afghanistan. Depuis la fin des années 2000, la plupart des armées occidentales se sont penchées sur l'intégration toujours plus étroite du facteur humain dans l'analyse du terrain où leurs troupes se déploient. De par la multiplicité des données employées et la complexité de leurs combinaisons, intégrer la géographie humaine au processus de production géographique militaire est un défi différent de ceux relevés précédemment pour l'intégration des données de géographie physique. La géographie humaine comprend l'étude des frontières internationales, des frontières tribales, des mouvements nomades, des affiliations religieuses, de l'idéologie politique, des taux de natalité et de mortalité, des lieux peuplés, de la proximité des établissements de santé, des principaux produits de base du marché, de l'ethnicité et des langues associées, ainsi que d'autres couches de données culturelles. Anciennement connue sous le nom d'analyse régionale, la géographie humaine étudie l'activité humaine, avec une référence particulière à la localisation, ainsi que les causes et les conséquences de cette activité [338]. L'Irak et l'Afghanistan ont donc été le terrain d'expérimentation concernant l'implémentation de la géographie humaine, en remettant au centre des débats militaires la question de la lutte contre-insurrectionnelle pour la première fois depuis la fin de la Guerre froide. La création par l'armée américaine du *Human Terrain System* en 2006[339], a permis la mise en place d'une première méthodologie dans la capture et l'analyse de données de géographie humaine sur ces théâtres d'opérations contemporains. Mis en place entre 2007 et 2014, ce dernier a depuis été retravaillé et intégré au manuel du personnel de la NGA sous le terme de *Human Terrain Analysis*. Si le développement de cette méthode a ouvert une nouvelle ère dans l'intégration de la géographie humaine

---

336 Chirio Maud, « Le pouvoir en un mot : les militaires brésiliens et la « révolution » du 31 mars 1964 », in *Nuevo Mundo, Mundos Nuevos*, n°7, 2007.

337 Galula David, « Contre-insurrection théorie et pratique », Paris, Economica, 2008.

338 Eunice P., « Human Geography Depicts Cultural Terrain », Pathfinder, Vol. 8, No. 5, 2010.

339 Kipp Jacob, Lester Grau, Prinslow Karl et coll., « The Human Terrain System », Military Review, sept.-oct. 2006.

au sein des armées, sa généralisation au sein de l'ensemble des armées occidentales n'a pas été automatique.

La définition d'une méthodologie en géographie humaine se heurte à de nombreuses difficultés, concernant l'extrême abondance de données et leur très grande hétérogénéité, qui nécessite un grand nombre de personnels aux compétences très variées (géographie, Histoire, sociologie, ethnographie…), mais également concernant le manque d'information sur la zone et les populations qui l'habitent, un problème récurrent dans le cadre d'un déploiement militaire à l'étranger. Cette complexité inhérente à la géographie humaine explique que, de tous les domaines de la géographie, c'est celui qui ait reçu le plus tard l'attention du monde de la normalisation, même dans le domaine militaire. Cependant, le besoin en géographie humaine n'a cessé de croître ces dernières années, menant à la multiplication de sociétés privées offrant des services dans ce domaine, à différentes échelles, et à la méthodologie parfois obscure. Un premier programme mené par les Américains a vu le jour en 2017, le World-Wide Human Geography Data Working Group, rassemblant une centaine de pays, dans le but de produire une base de données globale en matière de géographie humaine. Parmi les programmes nés à la suite de la création du WWHGD, l'International Program for Human Geography (IPHG) a été conçu comme le dernier-né des programmes de coproduction militaire, fondée sur le même modèle que MGCP/MUVD, dans le but de proposer des produits de géographie humaine normalisés, réutilisables et interopérables, exploitables dans un contexte d'engagement en coalition. Fondé en 2020, le programme IPHG est composé en 2023 de 18 pays, dont la France[340]. Les produits du programme IPHG sont peu nombreux du fait de la jeunesse du programme et des sessions d'entraînement visant à former les techniciens en charge de produire ces données sont encore régulièrement organisées pour toutes les nations membres.
Face à la complexité des données de géographies humaines et à l'extrême variété des produits qu'il est possible de créer dans le cadre d'un programme portant sur la géographie humaine, la NGA a décidé de limiter les productions IPHG à trois thèmes distincts : la langue, la religion et l'ethnicité. Ainsi, l'ensemble des cartes achevées dans le cadre du programme IPHG portent sur un ou plusieurs de ces éléments. À titre d'exemple, la France a ainsi produit une carte de la répartition ethnique dans la corne de l'Afrique (Somalie, Djibouti, Érythrée et Éthiopie). Si cela constitue indéniablement un aspect fortement limitant quant à la richesse des productions IPHG, une telle décision a tout du moins le mérite de fixer un cadre clair quant à la portée des produits demandés. Cela facilite également l'analyse de la complexité des travaux effectués, et par extension, le calcul des crédits obtenus qui ouvrent la possibilité aux nations membres de récupérer les produits créés par les autres nations. Le programme

[340] Les pays membres du programme IPHG sont : Australie, Brésil, Canada, Danemark, France, Allemagne, Grèce, Lituanie, Pays-Bas, Nouvelle-Zélande, Norvège, Roumanie, Afrique du Sud, Espagne, Turquie, Royaume-Uni, États-Unis, Japon.

IPHG ouvre donc un champ très prometteur dans la coopération internationale en matière de production de données géographiques pour les armées. Son ambition, pour l’instant modeste en termes de complexité, se devront probablement d’être rapidement interrogés une fois les projets de chaque nation livrée. Une extension de ce programme à des thèmes plus complexes pourrait ouvrir des perspectives très intéressantes en matière de partage de données de géographie humaine à l’échelle internationale et, si ce dernier est destiné à perdurer dans le futur, cela deviendra probablement nécessaire à plus ou moins long terme, sous peine de voir l’intérêt des nations participantes retomber face à l’investissement en personnel et financier nécessaire au fonctionnement de ce programme.

Conclusion du Chapitre II

Tant dans le domaine civil que militaire, l'écosystème international de la normalisation des données géographiques est caractérisé par son aspect multiscalaire, et s'articule autour d'organisation régionale et internationale, dont les acteurs à la fois publics et privés collaborent et s'opposent pour développer les technologies futures en matière de production et de diffusion de ces informations. De par leur importance et l'étendue des domaines s'appuyant sur ces informations, les acteurs de cet écosystème sont variés et présentent des intérêts divergents qui se répercutent sur la façon dont s'organisent les différents instituts de normalisation. Si l'ISO occupe une place importante au sein de cet écosystème de par la portée internationale de ses normes et la renommée des travaux qui y sont menés, il ne faudrait pas oublier l'importance des consortiums privés, tels que l'OGC. De par l'extrême richesse des sociétés privées gravitant autour de la production et de l'exploitation des données géographiques, l'OGC constitue aujourd'hui le fer de lance de l'innovation en matière de normalisation dans ce domaine. Le poids de sociétés, telles que Google, Esri, Airbus Defense and Space ou d'organismes comme l'IGN, participent directement à modeler l'environnement international en matière de production et d'échange de données géographiques numériques. Renforcer la présence française au sein de l'OGC doit constituer pour la France une priorité si elle souhaite continuer à avoir droit au chapitre sur la façon dont l'environnement des données géographiques numériques est modelé. En particulier, concernant le développement des nouvelles technologies appliquées aux données géographiques numériques, telles que l'IA ou l'Internet des objets. Si les nations européennes, aux premiers rangs desquels la France, occupent une place dominante au sein de ces institutions du fait d'un avantage historique et d'un investissement important, la pérennité de cette position s'explique également en grande partie par la fondation de l'Union européenne et des agences régionales de normalisation qui apportent aux pays de l'espace européens des espaces de négociations privilégiés afin de coordonner leurs propositions. À cela s'ajoute la prédominance des lois européennes, notamment en matière de normalisation, sur les lois nationales au sein de l'Union, qui permet de garantir l'unicité normative du marché européen des données géographiques numériques lorsque les normes sont traduites dans la loi. Ces lois permettent de faciliter au sein de l'Union le développement de projets géographiques transfrontaliers essentiels aux projets transnationaux concernant la gestion du territoire de l'Union et la préservation de la souveraineté de ses pays membres. Ces programmes, qui portent notamment sur la gestion des espaces transfrontaliers, comme la gestion des Alpes entre la France et l'Italie, contribuent à la préservation de la bonne entente entre les États européens et au règlement des différends frontaliers qui ont subsisté en Europe bien après la fin de la Seconde Guerre mondiale. Il est

donc d'une importance capitale que la France ne ménage pas ses efforts pour maintenir, voire améliorer sa position, au sein de ces instances européennes, qui constituent un échelon essentiel pour appuyer ses propositions de normes à l'international. Le domaine civil et militaire est également interconnecté concernant la normalisation des données géographiques numériques. Si les armées ont leurs propres besoins et leurs propres circuits internes pour choisir les normes à adopter, elles sont également dépendantes des avancées technologiques faites au sein des institutions civiles, notamment l'OGC, qui sont souvent au premier plan en matière d'innovation dans ce domaine. En tant que membre de l'OTAN et du DGIWG, la France développe ses normes en collaboration avec ses alliés et sa capacité à être, un acteur actif de ces processus est essentiel dans la défense de ses intérêts. Si les intérêts nationaux restent la priorité concernant le développement de ces normes, l'interopérabilité des armées françaises avec leurs homologues alliés, lors des déploiements en coalition, est un facteur qu'il n'est pas possible d'ignorer. Le développement des programmes de coproduction se fait dans cet esprit et apporte à la France et à ses alliés une quantité de données normalisées que les seuls programmes d'interopérabilité de l'OTAN ne pourraient garantir. Sans compter que ces programmes rassemblent des nations non présentes au sein de l'OTAN, et participent de la construction d'une communauté militaire élargie dans la production et la normalisation de données géographiques. L'ensemble de ces communautés sont entremêlées à différentes échelles, et rassemblent souvent les mêmes experts, même entre communautés civiles et militaires, renforçant le caractère endogamique de cette communauté mondiale de la normalisation des données géographiques numériques, avec tout de même un certain tropisme occidental.

Dans le troisième chapitre de cette première partie, seront abordés les enjeux spécifiques à ces différents acteurs et communautés d'intérêts prenant part à la normalisation des données géographiques numériques. Dans un premier temps seront décrits les enjeux des acteurs étatiques, puis ceux des acteurs privés. Enfin, la question des enjeux spécifiques de la communauté militaire fera l'objet d'un approfondissement particulier.

Chapitre III - Les enjeux de la normalisation des données géographiques

1. Les Enjeux des acteurs étatiques

1.1 Un investissement essentiel pour l'État

L'acquisition de données géospatiales numériques représente pour les administrations publiques une charge financière importante, que le coût élevé des opérations de terrain, de l'imagerie satellitaire et des infrastructures de traitement contribue à alourdir. Cette contrainte budgétaire a conduit les organismes publics à inscrire la réutilisation et le partage de données au cœur de leurs pratiques, dès lors que les ensembles collectés peuvent répondre à des objectifs de mission variés. La normalisation technique joue ici un rôle de crucial. En effet, en centralisant la conception de l'architecture de l'information, elle permet de décentraliser la production, la maintenance et le développement des outils logiciels, rendant ainsi possible une division du travail entre organismes sans compromettre l'interopérabilité des données produites. Les travaux de Nedovic-Budic, Pinto et Warnecke ont montré que les motivations qui poussent les administrations à partager leurs ressources géospatiales se répartissent entre convergence des missions institutionnelles d'une part, et recherche d'économies d'échelle d'autre part[341].

Au-delà de cette logique d'économie interne, l'ouverture des données géographiques poursuit des objectifs de politique publique plus larges. Comme le souligne l'étude de la NASA, les administrations y voient un levier important pour l'aide à la décision. La capacité de croiser et de recombiner des jeux de données issus de sources multiples permet d'identifier des dynamiques sociales, environnementales ou économiques qui resteraient invisibles si chaque organisme conservait ses informations en silo. La mise à disposition gratuite de données géospatiales de référence constitue ainsi une forme de production de bien commun numérique, dont le coût marginal de diffusion tend vers zéro dès lors que les infrastructures numériques sont en place. Elle réduit par ailleurs les coûts de transaction entre le secteur public et les acteurs privés qui les consomment. Cette ouverture n'est bien évidemment pas sans limite. Ainsi, les données relatives aux infrastructures critiques, telles que les réseaux d'eau

[341] Nedovic-Budic Zorica, K. Pinto Jeffrey, et Warnecke Lisa, « GIS Database Development and Exchange: Interaction Mechanisms and Motivations », *URISA Journal*, vol. 16, n° 1, 2004.

potable, les ouvrages d'art ou encore les installations électriques, sont diffusées de façon restreintes, pour tenir compte des risques que leur divulgation non contrôlée ferait peser sur la sécurité publique[342].

La logique économique du partage de données numériques repose sur une propriété fondamentale des biens informationnels, qui est que leur reproduction ne détruit pas la ressource initiale, comme l'avait déjà relevé en 2005 l'étude menée par Booz Allen Hamilton pour la NASA. Ainsi, lorsqu'un producteur de données géographiques met ses fichiers à disposition d'un tiers, il n'en est pas privé pour autant[343]. En termes d'analyse économique, ce transfert satisfait au critère d'amélioration tel que défini par Pareto : le destinataire voit sa situation s'améliorer significativement, tandis que le producteur original n'est en rien pénalisé[344]. À titre d'exemple, un organisme tel que la DREAL Grand Est, disposant d'un référentiel topographique récent pour son territoire, peut le mettre à disposition du conseil régional sans qu'il cesse d'être exploitable pour ses propres missions. La valeur nette de l'opération est strictement positive pour la collectivité dans son ensemble, et nulle pour le producteur. Cette propriété structure en profondeur les stratégies de mutualisation de données géospatiales au sein de l'écosystème public français. Elle justifie par ailleurs que de nombreuses administrations aient adopté des politiques tarifaires fondées sur le seul coût de reproduction, soit aujourd'hui la quasi-gratuité, plutôt que sur le recouvrement intégral des frais de production.

De multiples niveaux de gouvernement s'engagent de diverses manières dans l'univers des normes géospatiales comme le décrit également l'étude de Booz Allen Hamilton. En effet, l'État est à la fois *« un utilisateur, un défenseur et un fournisseur de ressources »*[345]. Le gouvernement intervient également pour remédier aux défaillances du marché et pour protéger la santé et la sécurité publiques lorsque le marché n'est pas incité à le faire. Les gouvernements ont donc un rôle établi dans le financement de la production de biens publics et dans la correction des lacunes lorsque les marchés commerciaux ne parviennent pas à fournir ces biens. Cependant, les motivations des gouvernements à différents niveaux pour adopter des normes varient, et les normes qu'ils adoptent peuvent varier.

Selon la même étude, l'État doit jouer un rôle actif dans la protection des droits de propriété intellectuelle et dans la promotion des biens communs de l'information. Il existe des incitations économiques contradictoires qui poussent l'industrie privée à breveter les normes et à s'emparer des flux de revenus associés à l'utilisation de la technologie. Il existe également plusieurs préoccupations

[342] Booz Allen Hamilton, « Geospatial Interoperability Return on Investment Study », National Aeronautics and Space Administration, Geospatial Interoperability Office, avril 2005, p. 33.
[343] Booz Allen Hamilton, « Geospatial Interoperability Return on Investment Study », National Aeronautics and Space Administration, Geospatial Interoperability Office, avril 2005, p. 30.
[344] National Research Council, « Licensing Geographic Data and Services », The National Academy of Sciences, p. 10, 2004.
[345] Booz Allen Hamilton, « Geospatial Interoperability Return on Investment Study », National Aeronautics and Space Administration, Geospatial Interoperability Office, avril 2005, p. 40.

liées au brevetage des normes et des spécifications. La première préoccupation est le risque d'étouffer la collaboration. L'industrie est caractérisée par des acteurs hétérogènes qui exercent un pouvoir asymétrique. Ceux qui détiennent une grande part de marché et une position dominante sur le marché sont poussés à agir de manière opportuniste pour améliorer ou protéger leur position sur le marché. Le gouvernement peut jouer plusieurs rôles pour faciliter l'adoption de normes. Par exemple, établir des politiques claires en matière de propriété intellectuelle pour tous les participants, créer et diffuser des règles claires pour l'accès et la disponibilité des normes et des processus de création de normes, faciliter l'accès à l'information, réduire l'asymétrie d'information entre les participants, adopter uniquement des normes ouvertes, élaborées en collaboration ou encore participer et contribuer aux processus d'élaboration de normes ouvertes[346].

La puissance étatique se doit donc de se pencher sur les enjeux de souverainetés sous-jacents à la production, la diffusion et la normalisation des données géographiques. En effet, à l'heure de la révolution de l'information, les données géolocalisées occupent une position stratégique et ne doivent pas être négligées par la puissance publique, comme souligné par le rapporteur spécial de la commission des finances dans son dernier rapport sur l'IGN[347]. La capacité à produire des données géoréférencées de pointe en toute autonomie constitue aujourd'hui une garantie indispensable à l'exercice de la souveraineté nationale. Cette capacité de production ne peut s'accompagner d'une politique efficace en matière d'emploi de la donnée, uniquement si cette dernière s'appuie sur une normalisation efficace, condition indispensable à la bonne réutilisation des données. Le paysage des données géolocalisées est vaste, et rassemble une diversité d'acteurs tant publics que privés, aux logiques de fonctionnement parfois contradictoires. Avec la refondation du système de financement de l'IGN en 2019, et l'approfondissement du rôle des échelons infranationaux dans la logique de production de données géographiques, en particulier à l'échelon régional [348], la coordination de l'ensemble de ces acteurs au sein de l'écosystème normatif des données prend une importance capitale. Il revient à l'État la charge de se pencher sur cette question, afin d'assurer l'interopérabilité des différents acteurs impliqués s'il souhaite tirer pleinement parti de la production de ces données stratégiques que sont les données géoréférencées.

---

346 Booz Allen Hamilton, « Geospatial Interoperability Return on Investment Study », National Aeronautics and Space Administration, Geospatial Interoperability Office, avril 2005, p. 33

347 Vincent Capo-Canellas, « Rapport d'information fait au nom de la commission des finances sur l'Institut national de l'information géographique et forestière (IGN) n° 17 », Sénat, 5 octobre 2022.

348 Loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République.

2. Le rôle des acteurs privés : entre risque et recherche d'avantage compétitif

Comme les gouvernements, l'industrie est une vaste catégorie qui comprend plusieurs secteurs technologiques. Ces secteurs comprennent les vendeurs de convertisseurs de données et les vendeurs de logiciels géospatiaux, les technologies géospatiales de soutien (par exemple, GPS et identification par radiofréquence), les fournisseurs d'imagerie par télédétection et d'autres entreprises commerciales auxiliaires. Au contraire, certains secteurs de l'industrie sont complètement indifférents aux normes (par exemple, les vendeurs de convertisseurs de données). Aujourd'hui (2026), la France compte 581 sociétés impliquées dans l'exploitation et/ou la collecte d'informations géographiques [349]. Parmi ces sociétés, près de 90 % d'entre elles sont des TPE/PME. L'étude de Booz Allen Hamilton souligne également comment certaines entreprises du domaine des technologies géospatiales considèrent le soutien des produits aux normes et aux spécifications de l'Information géographique comme un facteur de démarcation sur le marché. Ces fournisseurs affirment qu'ils offrent un service supérieur aux produits propriétaires à un coût moindre. Ils considèrent que leur avantage sur le marché est de pouvoir offrir à leurs clients une certaine transparence dans le cadre de la création de leur gamme de services [350]. Les entreprises qui misent sur les normes géospatiales font le pari qu'elles seront adoptées et que leur produit deviendra un élément indispensable de l'infrastructure d'exploitation informatique. Pour ces entreprises, la sensibilisation, la crédibilité, la fidélité au produit et le capital intellectuel accessible par l'adoption de normes transparentes sont le chemin vers l'omniprésence et, par conséquent, la part de marché. Cette position représente une différence marquée par rapport à la position plus traditionnelle de la concurrence sur le marché en offrant des modèles de données propriétaires, des interfaces d'application et des services associés.

Cependant, l'étude révèle aussi que la participation aux activités d'élaboration de normes comporte certains risques pour l'industrie, que tous les acteurs cherchent à minimiser. Participer à des activités de normalisation sans divulguer une intention propriétaire (intérêt ou intention de déposer un brevet) peut être considéré comme frauduleux et peut aboutir à un brevet inapplicable. Les règles antitrust de l'OGC exigent la divulgation des intérêts matériels dans les spécifications brevetables avant le vote sur les mesures techniques. Dans certains cas, cependant, les détenteurs de brevets acceptent de ne pas payer de redevances ou de payer des redevances très faibles pour l'utilisation de méthodes et de

[349] Site Internet de l'association GeoRezo : https://georezo.net/geo-entreprise/index.php?mode=random&keyword=&activite=&specialite=&region=&departement=&page=1&limit=1000#results

[350] Booz Allen Hamilton, « Geospatial Interoperability Return on Investment Study », National Aeronautics and Space Administration, Geospatial Interoperability Office, avril 2005, p. 31

technologies exclusives, ce que l'on appelle des conditions « raisonnables et non discriminatoires » ou RAND (Reasonable and Non Discriminatory)[351]. Dans chaque cas, cela dépend de la position de l'entreprise ou du secteur technologique sur le marché.

L'étude de Booze Allen Hamilton révèle également qu'une autre question qui se pose est celle du financement privé des biens publics. Contrairement aux organisations internationales de normalisation (comme par exemple l'ISO), l'adhésion aux consortiums privée est relativement coûteuse et n'est ouverte qu'à ceux qui peuvent se le permettre[352]. Cette adhésion limitée a pour effet de développer des normes financées par le secteur privé qui deviennent des biens dits « de club », comprendre ici des biens réservé à un groupe restreint d'acteurs entretenant des relations entre eux. De nombreuses entreprises considèrent l'adhésion à un consortium comme un moyen de « payer pour jouer » dans l'espoir d'obtenir un avantage concurrentiel. Peut-être parce que le secteur de la technologie géospatiale est relativement petit par rapport à l'industrie plus vaste de la technologie de l'information, le développement des normes géospatiales est dirigé autant par les petits acteurs de l'industrie que par les grands. De plus, l'OGC dispose de plusieurs catégories de membres associés et de membres commerciaux de petites entreprises qui permettent une participation accrue des petites entreprises, des organisations à but non lucratif et des organisations universitaires.

Il faut aussi noter que les fournisseurs de logiciels SIG soutiennent de plus en plus les normes géospatiales. L'étude de la NASA le soulignait déjà en 2005, ESRI, Intergraph et MapInfo soutiennent tout un mélange de spécifications de l'OGC. L'utilisation généralisée des normes ouvertes dans la communauté géospatiale a un impact sur toutes les entreprises de ce secteur. Les organisations qui sont les plus touchées sont les fournisseurs de logiciels SIG. Actuellement, la majorité de ces fournisseurs prennent en charge les normes ouvertes dans le cadre de leur gamme de produits. La demande de solutions basées sur des normes sur le marché national et international implique que, pour les leaders du marché dans les différentes catégories de SIG, il y a deux solutions : bloquer l'adoption de normes ouvertes ou fournir des solutions qui respectent et dépassent les normes. Actuellement, aucun des leaders de l'industrie n'a ouvertement dénoncé le mouvement des normes géospatiales au sein de la communauté SIG. De plus, tous les leaders du marché sont membres de l'OGC[353].

[351] Booz Allen Hamilton, « Geospatial Interoperability Return on Investment Study », National Aeronautics and Space Administration, Geospatial Interoperability Office, avril 2005, p. 32
[352] Ibid p.32
[353] Ibid, p. 32

3. Les enjeux de la normalisation des données géographiques pour les acteurs militaires

3.1 La production géographique au sein des armées

La connaissance du terrain est un des aspects les plus fondamentaux de la conduite de toute opération militaire. L'importance du terrain dans la planification et la conduite de la guerre a été saisie par les stratèges dès la plus haute antiquité. De ce fait, le stratège chinois *Sun Tzu*, dans son *Art de la Guerre* plaçait déjà le terrain et les conditions météorologiques au nombre des cinq facteurs fondamentaux dans l'évaluation de la guerre, au même niveau que l'influence morale, l'autorité et la doctrine [354]. Si ce terrain est longtemps décrit de façon laconique comme *« les lieux où se déroulent les opérations militaires »* [355], dès le XIXe siècle, les évolutions technologiques en matière de transport terrestre, nautique et aérien ainsi qu'en matière de communication vont provoquer une révolution dans la perception du terrain et introduire la notion d'espace, avec sa dimension spatio-temporelle, dans le vocabulaire militaire. Qualifié de *géographique* dans la doctrine officielle d'emploi des forces au sein de l'armée française, l'espace géographique constitue le concept fédérateur de l'ensemble des termes relatifs au milieu. Le premier aspect pris en compte par le milieu militaire lorsque l'on parle de géographie est la géographique physique. De fait, la réalité physique du terrain, avec ce qu'elle implique de contrainte et de possibilité, à la fois pour les forces alliées et ennemies, constitue le premier aspect à prendre en compte pour la militaire. L'aspect topographique du terrain, avec ses obstacles naturels et artificiels, la nature de ses sols, et, d'une manière générale, sa forme est donc d'une importance cruciale. Ce dernier influe à la fois sur les vues, les couverts, l'efficacité des feux, les voies de passage pour les hommes et les matériels ou encore les abris disponibles à l'ensemble des belligérants. Il faut également prendre en compte le climat qui influe directement sur le comportement des systèmes d'armes et des hommes engagés sur le terrain. Cependant, la connaissance de ces données ne suffit pas, il est également nécessaire au militaire de pouvoir analyser ce terrain afin de déterminer les répercussions exactes que ce dernier aura sur le déploiement des unités militaires, des effets qui varient non seulement en fonction du terrain, mais également des objectifs à accomplir sur le champ de bataille (par exemple, si l'on est assaillant ou défenseur). L'acquisition de données topographiques et la

[354] CDEF et DREUX, « Géographie et combat en zone urbaine », in *Cahier de la recherche doctrinale*, Centre de doctrine d'emploi des forces, janvier 2005.

[355] *Ibid*

constitution de cartes ou de modèles numériques de terrain constituent donc une étape essentielle de la préparation d'une opération militaire, en ce qu'elles fournissent les conditions sine qua non à l'analyse du terrain. Il est à noter que ces notions s'appliquent autant aux terrains étrangers sur lesquels les troupes françaises sont susceptibles de se déployer, que le territoire national qu'il leur incombe de défendre. Les facteurs météorologiques sont également à prendre en compte, ces derniers peuvent imposer des contraintes très fortes aux combattants et à leur matériel, en réduisant leur visibilité, leur mobilité, en leur imposant des contraintes logistiques fortes. La guerre en Ukraine est ici un parfait exemple de ces contraintes. Le déclenchement de la guerre s'est fait à la fin de l'hiver 2022, qui offre un climat favorable aux hommes et aux véhicules pour lancer de grandes offensives. Tandis que l'automne a vu les deux armées réduire significativement leurs mouvements, le climat ukrainien ayant transformé de larges parties du front en océans de boues rendant le mouvement des véhicules très compliqués et empêchant de ce fait les grandes offensives mécanisées. Au contraire, l'hiver qui apporte avec lui son lot de contraintes pour les hommes engagés, a également permis la reprise du mouvement en gelant les espaces auparavant boueux, déclenchant une nouvelle phase de manœuvre. Aujourd'hui l'acquisition d'information météorologique rendue possible par les centres nationaux de météorologies est essentielle à la maîtrise de l'environnement de combat et rentre en compte dans la préparation géographique des armées.

L'ensemble des données géographiques et météorologiques sont exploitées via un certain nombre de produits au premier rang desquelles se trouve la carte. Les produits cartographiques qu'ils soient papiers ou numériques constituent l'épine dorsale de l'exploitation des informations géographiques. Ces dernières sont le support d'une information synthétisée, transformée en symboles, et apportent sous la forme d'un format adapté à la compréhension humaine l'ensemble des informations nécessaires, et uniquement celles-ci, sur les éléments naturels et anthropiques du terrain nécessaire à tous les échelons, du stratégique aux tactiques. La géographie numérique au service des forces armées s'est développée dès les années 1960 avec le développement des premiers satellites américains. Les premières SIG, quant à eux, datent des années 1980 et ont été immédiatement mises au service des armées dans la production de carte [356]. Le développement de la production de données géographiques numériques a également directement influencé à partir des années 1990 le développement de nouveaux systèmes d'armes au sein de toutes les armées, s'appuyant sur ces données géographiques. Le développement de ces nouveaux outils technologiques et l'émergence d'une nouvelle capacité de production de données géographiques encore jamais vu auparavant, va façonner la façon dont les États vont concevoir la place de la géographie au sein de leur stratégie de défense. Si l'accès aux données géographiques numériques se démocratise rapidement au sein des armées occidentales, les avancées

[356] Desbois Henri, « La carte et le territoire à l'ère numérique », *Socio*, n° 4, 2015.

technologiques ne résolvent pas pour autant l'ensemble des problèmes auxquels font face les armées. Tout d'abord les coûts de production restent relativement élevés, les connaissances nécessaires à l'élaboration de cartes précises en dehors du théâtre ouest européens restent largement manquantes et la simple acquisition d'images satellites, d'une qualité souvent médiocre avant les années 2010, ne permettent pas de remédier à ces problèmes. Or, la fin des années 1990 et l'entrée dans un monde post-guerre froide est marqué pour les armées occidentales par la nécessité de se déployer sur des théâtres d'opérations sur lesquels les informations géographiques sont souvent datées, comme en Afrique ou au Moyen-Orient. Si le développement de la géographie numérique révolutionne donc l'emploi de la géographie au sein des armées, elle ne résout pas pour autant l'ensemble des problèmes posés par les nouveaux défis de la guerre au XXIe siècle.

Un problème persistant pour les armées occidentales tient également à l'interopérabilité des données entre alliés, les interventions en coalition atteignant alors un niveau jamais vu depuis la fin de la Seconde Guerre mondiale. Les armées font souvent face à des problèmes de compatibilité entre les différents systèmes et logiciels informatiques employés, qui ralentissent voire empêchent l'échange d'informations géographiques entre elles. Il faut également rajouter à cela les systèmes de géoréférencement parfois imprécis, qui freinent le développement de systèmes d'armes qui requièrent toujours plus de précisions. De plus, les développements technologiques en matière d'acquisition de données complexifient toujours plus le problème de l'échange de données. La fin des années 90 voit la multiplication des plateformes d'acquisition de données, qu'il s'agisse des drones aériens, sous-marins, des satellites toujours plus performants ou encore de véhicules spécialisés dans la saisie topographique pour les unités engagées sur le terrain. Tous ces développements entraînent progressivement le remplacement des données géographiques analogiques par des données numériques comme principaux outils d'aide à la décision au sein des armées, bien que les cartes analogiques ne disparaissent jamais complètement, leur rusticité garantissant leur maintien au sein des forces armées. Il faut ajouter à cela le développement de nouveaux types de données dans les années 2000, comme les cartes vecteurs, les modèles numériques de terrain (MNT), de surface (MNS) et d'élévation (MNE) et le développement de la 3D[357]. Les données vecteurs se développent également avec l'aide des données raster orthorectifiés servant de fond de carte. Enfin, dans le même temps, le développement des systèmes d'armes intégrant de la donnée géographique renforce le besoin en données géographiques numériques. Comme précisé au début de cette étude, les acteurs militaires ont saisi depuis longtemps la nécessité d'organiser la normalisation des produits employés, et ce, dans tous les domaines techniques. En France, les armées disposent du Centre de normalisation de Défense (CND), en charge de la négociation des STANAGs auprès de l'OTAN, mais également des accords de normalisation avec les industriels de la défense en

[357] Boulanger Philippe, « La géographie reine des batailles », Perrin, 2020.

charge de fournir les armées en matériels dont il faut assurer en permanence l'interopérabilité avec les normes en vigueur.

Afin de pallier au manque d'interopérabilité entre les différents systèmes de géoréférencement au sein des armées occidentales (ainsi, le datum [358]anglais OSGB36 diffère du datum européen ED50 d'environ 200 mètres), l'OTAN décide dans les années 2000 d'utiliser le transverse universel de Mercator (UTM) et l'ED50 pour son système de référence de coordonnées militaire. Le système ne convient pas parfaitement aux besoins français, puisque l'IGN utilise toujours le système Lambert II qui nécessite de superposer la grille UTM par-dessus afin d'avoir un référencement exact. La prédominance américaine au sein de l'OTAN a garanti l'adoption de cette norme au sein de l'Alliance atlantique. Cependant il n'existe pas de référentiel unique pour l'ensemble des données échangées.

Les besoins des armées en matière de production de données géographiques sont anciens, et se distinguent du milieu civil par leur finalité : la conduite des opérations. L'information géographique est avant tout un moyen pour les militaires de se positionner, de connaître leur environnement d'engagement, mais également pour se coordonner et exploiter leurs différents systèmes d'armes. En effet, aujourd'hui, près de 90 % des systèmes d'armes employés par l'armée française exploitent des données géographiques de différentes natures [359]. Les besoins opérationnels dans le domaine des géosciences militaires sont très difficiles à définir. Plusieurs facteurs clés doivent être pris en compte, notamment le degré d'avancement des solutions techniques par rapport aux besoins opérationnels réels, les cycles d'innovation rapides, les scénarios complexes, les fournisseurs de services spécialisés et les questions de sécurité et de confidentialité.

L'interaction entre un client/consommateur et son producteur/fournisseur de services est fondamentalement différente entre le monde civil ouvert et le domaine gouvernemental, en particulier dans les services de sécurité. La relation civile entre le client et son producteur, par exemple un fabricant de cartes, est principalement régie par les forces du marché, telles que l'offre et la demande, et s'exprime généralement sous la forme d'un certain prix pour le produit ou d'une redevance. Le monde gouvernemental, en revanche, est principalement mû par des tâches et des ordres et n'est pas régularisé principalement par les coûts associés.

Le fournisseur de géoservices pour la sécurité nationale ou les forces de défense doivent donc agir comme un facilitateur pour les troupes et fournir le produit nécessaire pour soutenir les scénarios définis par le cadre juridique et ne pas suivre l'offre et la demande. Les missions internationales, telles que celles menées sous l'égide de l'OTAN, de l'UE ou de l'ONU, présentent une complexité supplémentaire en termes d'exigences opérationnelles, car l'interopérabilité sur le terrain entre les

[358] Le terme de datum désigne la position d'un réseau géodésique sur la Terre.
[359] Entretien avec un ancien directeur du BGHOM, le 14 mars 2022.

forces nationales est indispensable à la réussite de la mission. Au cours des dernières décennies, l'homogénéisation des différents besoins militaires nationaux pour les opérations, y compris la géographie, a été réalisée au niveau national ainsi que par l'intermédiaire de l'OTAN et de l'UE (au travers de l'Agence européenne de défense et l'État-major militaire de l'Union européenne), mais les perspectives nationales priment toujours dans le processus décisionnel [360].

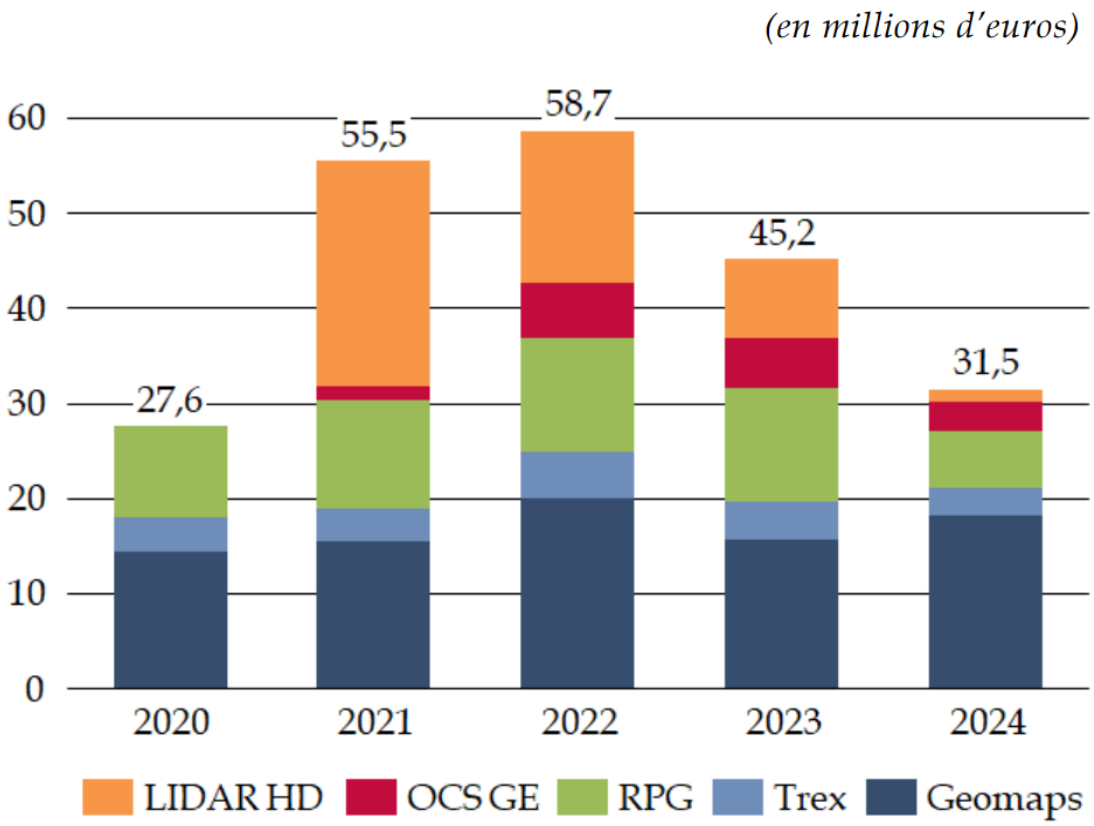
La France fait partie des rares puissances à disposer d'une chaîne complète de production de données géographiques entièrement autonomes, s'appuyant à la fois sur des acteurs publics historiques, au premier rang desquels se trouve l'IGN, mais également sur un tissu industriel dense dont les groupes Thales et Airbus Defense and Space sont le fer de lance. L'IGN est l'héritier direct du Service géographique de l'armée dissous en 1940, et occupe aujourd'hui une place à part dans le paysage de la production de données géographiques dans le monde, en étant un des rares instituts nationaux géographiques à remplir à la fois des missions civiles et militaires. Les relations entre l'IGN et les Armées sont réglées par un protocole signé en juin 2000. Ce protocole a été complété en 2015 lorsque les nouveaux statuts de l'IGN sont venus confirmer cette relation de symbiose entre les besoins militaires et l'Institut national, en précisant : *« dans l'intérêt de la Défense ou de la sécurité nationale et sur demande du ministre de la Défense, l'institut contribue à la préparation, au développement et à la mise en œuvre de l'infrastructure de données géographiques nécessaires pour l'exécution des missions des armées et des programmes du ministère de la Défense »* [361]. De fait, aujourd'hui, le ministère des armées représente un des principaux clients de l'IGN, aux côtés du ministère de l'Agriculture et de la souveraineté alimentaire, le premier ayant versé près de 22 millions d'euros à l'IGN pour la seule année 2024, dans le cadre des projets TREx et Geomaps 3 (cf. figure 10) [362].

[360] Teichmann Friedrich, « Current Technological Challenges and Innovative Approaches for Military Geo-Services from an Austrian Perspective », in *Military Geoscience: A Multifaceted Approach to the Study of Warfare, Advances in Military Geosciences*, Springer Nature Switzerland, 2022.

[361] Décret n° 2011-1371 du 27 octobre 2011 relatif à l'Institut national de l'information géographique et forestière (IGN), version en vigueur au 12 décembre 2015.

[362] Capo-Canellas Vincent, « Rapport d'information fait au nom de la commission des finances sur l'Institut national de l'information géographique et forestière (IGN) n° 17 », Sénat, 5 octobre 2022.

Figure 10 : Evolution prévisionnelle des recettes tirées des « grands projets » de l'IGN (2020-2024)



Source : *Commission des finances du Sénat (2022)*

En outre, comme certaines des missions auxquelles participent les armées françaises se font en coalition, l'interopérabilité est vitale. Il est donc de la plus haute importance que toutes les normes nécessaires (par exemple, le géodatum, le système de coordonnées, les projections cartographiques) soient respectées. Cela inclut également le domaine complexe des métadonnées, en particulier pour les services numériques, qui doit être traité et homogénéisé. L'adoption de normes communes, par exemple dans le domaine des géoservices, nécessite, entre autres, une vision claire, la volonté de faire des compromis, des connaissances techniques approfondies et du temps, les groupes de travail sur la normalisation, en particulier les groupes internationaux, ont besoin de perspectives à long terme. La conséquence de la mondialisation pour les fournisseurs de services géographiques est la nécessité de fournir des produits et des données dans le monde entier. Cela doit se faire dans des formats normalisés qui favoriseront l'interopérabilité entre les nations participant à des missions combinées.

La principale différence avec le secteur civil tient avant tout dans les besoins propres aux forces armées auxquels ces données doivent répondre qu'il s'agisse de critères de précision particulière, ou encore de métadonnées plus détaillées. En matière de normalisation les armées coopèrent de façon

étroite avec les instances civiles, en particulier l'IGN. C'est la Direction générale de l'armement (DGA) qui communique à l'IGN les besoins exprimés par les armées, les deux organismes étant liés par un accord depuis plus de vingt ans, afin que la normalisation des données géographiques à l'international puisse répondre aux besoins exprimés par les forces armées. Ainsi, dans le domaine de la normalisation géospatiale, le monde civil, et en particulier celui des consortiums privés comme l'OGC, donne le tempo de l'innovation. Loin de chercher à réinventer la roue, donc, le monde militaire fait plus office de suiveur dans le domaine de la normalisation des données géographiques, en veillant toutefois à faire relayer ses besoins par les représentants civils au sein des organes de normalisation internationaux, comme l'ISO ou l'OGC.

La délimitation des besoins des armées en matière de production de données géographiques fait l'objet d'une grande attention au sein du ministère des armées (figure 11). Le processus décisionnel présidant aux choix des zones géographiques prioritaires mêle un certain nombre d'acteurs clés publiques et privées qui forment l'ossature de la production de ces données. Tout d'abord, au sein du ministère des armées, le commandement pour les opérations interarmées (CPOIA) et le bureau géographie hydrographie océanographie et météorologie (BGHOM) collaborent afin de définir les besoins opérationnels. L'établissement géographique interarmées (EGI) gère la production interne de données géographiques et met à disposition le stock de données déjà produites[363]. Ces données répondent le plus souvent à des impératifs normatifs liés à aux programmes de coproductions auxquels la France participe, ainsi qu'aux normes de l'OTAN. Enfin, toujours aux ministères des armées, la Direction générale de l'armement (DGA) est en charge de la rédaction des contrats qui lient les armées et les maîtres d'œuvre industriels impliqués dans ces productions géographiques. En effet, la France a organisé sa production de données géographiques militaires de façon à stimuler au maximum son tissu industriel, en se reposant sur une base industrielle et technologique de défense (BITD) dont Thales et Airbus Defense and Space sont les fers de lance, accompagnés de diverses PME. L'Institut géographique national fournit également un appui indispensable aux militaires en supervisant, grâce à sa longue expérience en la matière, les chantiers de production de données géographiques.

[363] Site officiel du ministère des armées : https://www.defense.gouv.fr/ema/commandement-operations-interarmees-cpoia

Figure 11 : Architecture de production de données géographiques au sein des armées

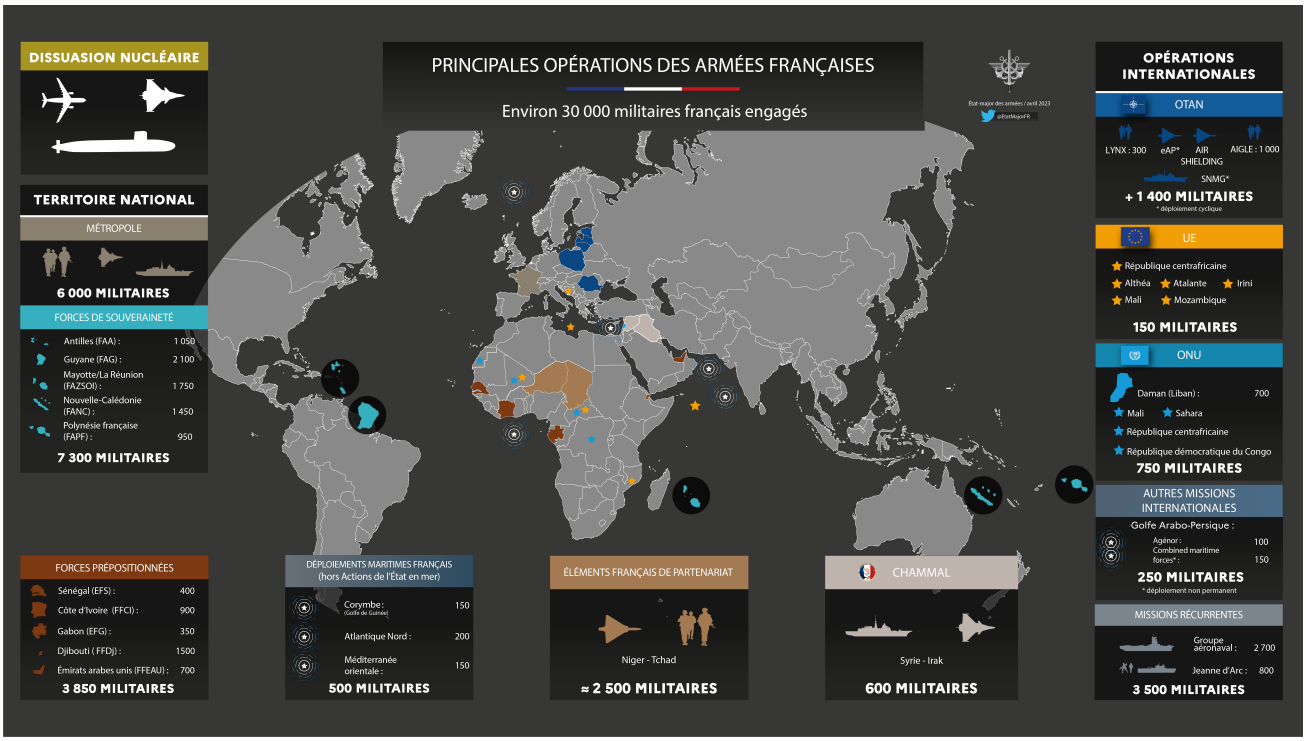


Source : *Ministère des armées (2022)*

Les besoins en matière d'information géographique sont particulièrement aigus pour l'armée française, qui reste une des armées occidentales les plus largement déployées à l'étranger. Ainsi, en 2023 l'armée française est présente dans près de 15 pays différents répartis sur tous les continents (voir figure 12)[364]. Autant de terrain d'opérations pour lequel des informations géographiques doivent être fournies. Le fournisseur national ou militaire de géoservices a la lourde tâche de fournir le paquet standard nécessaire au soutien des unités sur le terrain, y compris les cartes et les données géospatiales adéquates, en ce qui concerne les armes et les systèmes de navigation pour l'ensemble de ces régions. Il en résulte un besoin géoactuel de fournir des produits et des données pour une zone d'intérêt quasi globale, et pas seulement pour une ou deux zones prédéterminées. Cette multiplication des zones d'opération rend également l'anticipation des besoins en matière géographique d'autant plus complexe.

[364] Site officiel du ministère des Armées : https://www.defense.gouv.fr/operations/operations

Figure 12 : principales opérations des armées françaises



Source : *Ministère des Armées (2022)*

Ainsi, l'IGN et les armées entretiennent une relation très forte et de longues dates, le premier puisant dans les contrats du second une manne monétaire devenue indispensable à son fonctionnement, tandis que les armées s'appuient sur l'IGN pour sa grande expertise ainsi que son personnel très qualifié. De plus, en matière de normalisation, les travaux sont majoritairement dirigés par des civils issus de l'Institut géographique national. Qu'il s'agisse de l'ISO ou du DGIWG, les représentants français sont avant tout des civils, le BGHOM ne disposant pas de suffisamment de personnel qualifié dans ce domaine pour représenter les armées au sein des diverses organisations de normalisation civiles ou militaires. Ainsi, même au sein de l'OTAN où des réunions concernant les programmes de coproduction militaires, la majorité des représentants français restent des civils. Cependant, le travail des armées en la matière ne s'arrête pas là. Afin d'assurer un développement cohérent des normes géographiques dédiées à la Défense, les instances internationales, telles que l'ISO ne suffisent pas, ces dernières ne pouvant pas mettre en avant les besoins spécifiques des armées, et développent souvent des normes trop généralistes pour pouvoir répondre à ces besoins.

3.2 Les données géographiques militaires au défi de l'interopérabilité

Les défis opérationnels actuels pour les fournisseurs de données géographiques militaires peuvent être regroupés en plusieurs tendances. La mondialisation des zones d'opérations se traduit par une zone d'intérêt fondamentalement mondiale pour les nations et, pour l'interopérabilité entre les unités, nécessite des normes et des métadonnées appropriées pour les produits géospatiaux. L'accélération des échanges exige un processus décisionnel et un soutien géographique rapides, y compris un cycle d'innovation rapide en matière d'avancées technologiques. Avec la guerre moderne, d'autres facteurs géographiques pertinents apparaissent en rapport avec les nouvelles menaces, en particulier concernant l'aspect cyber des conflits. Le contrôle budgétaire implique la maîtrise des coûts des géoservices et exige des solutions innovantes et des synergies entre les acteurs sur le terrain. La numérisation comprend la transformation de l'analogique au numérique, avec de nouvelles opportunités, telles que les simulations et la réalité virtuelle, et les développements futurs dans le domaine du transfert de machine à machine, du Big Data et de l'exploitation des données, en particulier avec l'intelligence artificielle. La géographie et l'espace devraient établir un lien étroit, car la navigation par satellite et les solutions de positionnement, de navigation et de synchronisation sont essentielles pour les géoservices de pointe, en outre, l'observation de la Terre et la télédétection sont des éléments essentiels pour les géoproduits modernes. La grande complexité des missions modernes exige une approche globale, y compris la coopération et les partenariats, et favorise la mise en commun et le partage.

Les produits conçus par les ingénieurs géospatiaux vont des cartes aéronautiques et nautiques aux cartes topographiques, en passant par les produits de soutien au ciblage de précision, les modèles et systèmes géodésiques et géophysiques, mais également des rapports et notes de renseignement. Ils comprennent des produits standardisés et des produits personnalisés à des fins spécifiques [365]. Il s'agit généralement de produits en deux dimensions, tels que des cartes, des graphiques et des orthophotos, produits à l'aide de données géospatiales et de capteurs électro-optiques. Ces produits peuvent inclure des couches d'information supplémentaires issues du renseignement militaire. Ces produits standards servent de base à l'élaboration de produits plus personnalisés qui répondent aux besoins uniques des utilisateurs. Les produits spécialisés intègrent des données multicapteurs, des données de renseignement et des données géospatiales. Des affichages dynamiques en 3 et 4 dimensions et des produits interactifs adaptés aux besoins spécifiques des utilisateurs peuvent être créés à partir de ces technologies avancées, y compris des visualisations en vol et d'autres simulations de mission, en

[365] The Geospatial-Intelligence Standards Working Group (GWG), « Geospatial Intelligence standard : Part 2 : Overview of GEOINT Standards », On-line training modules sponsored by the Geospatial Intelligence Standards Working Group (GWG), 30 janvier 2007.

s'appuyant sur les modèles numériques de terrains produits en amont. Ces produits cartographiques sont soit produits en amont des opérations durant la phase précédant le déploiement ou directement sur le terrain grâce aux outils embarqués à la fois dans les véhicules de commandement ou à l'aide d'outils externes, comme des drones aériens, ou marins. Une fois les informations récoltées, ces dernières sont combinées grâce aux capacités des SIG afin de créer divers produits.

En France, la production de données géographiques militaires est divisée en plusieurs strates de complexité. Les données fondamentales dites données « socles » sont constituées de bases de données numériques sur la surface de la Terre, constituée à partir d'imagerie spatiale, des relevés des fonds marins conduits par la marine nationale et des modèles de prévision de la météo. La combinaison de ces informations physiques (terrestre et marines) ainsi que temporelles et climatiques permet la production de bases de données homogènes à partir desquelles sont bâtis les autres produits géographiques. Le programme GeoSocle s'appuie notamment sur les images satellites SPOT 6 et 7, Pléiades et Pléiades Neo (depuis 2021) fournis par Airbus Defense and Space d'une précision pouvant aller jusqu'à 30 cm. Il faut également y rajouter les satellites radars de la constellation radar de Airbus, ainsi que le satellite NovaSAR toujours chez Airbus Defense and Space. En fonction des besoins, l'armée peut également faire appel à d'autres satellites privés ou encore aux images des programmes satellites de l'Union européenne, tels que ceux du programme Copernicus. Le programme Geosocle permet ainsi la production d'un ensemble de données géoréférencées de référence pour la création de produits composés d'images aériennes, satellitaires et de modèles numériques de terrain, qu'il s'agisse de produits cartographiques ou de produits directement intégrés à des systèmes d'armes. Le programme GeoMaps, qui en est à sa troisième itération, est mené conjointement par les groupes Thales et Airbus Defense and Space et produit à partir de ces données des cartes allant de l'échelle 1/50 000e à l'échelle 1/5 000e dont les spécificités sont fondées sur les exigences des programmes de coproduction MGCP et MUVD. Un des avantages de la normalisation des données géographiques imposés par les programmes de coproduction tient notamment à la capacité de partage permise par ces exigences, qui s'imposent également aux produits cartographiques uniquement dédiés aux forces armées françaises. Ainsi, toutes les données produites dans le cadre du projet Geomaps peuvent potentiellement être partagées avec des nations alliées lors de déploiement en coalition. Ces dernières seront immédiatement interopérables avec les données produites par les autres participants au programme et dans un format exploitable par l'ensemble des systèmes d'information des nations alliés.

La tension induite par la portée quasi mondiale des opérations actuelles est multipliée par la nécessité d'un cycle de prise de décision rapide à tous les niveaux. Pour que l'opération soit couronnée de succès, la rapidité est essentielle. Par conséquent, le soutien géographique doit également fournir, idéalement en temps réel, toutes les données nécessaires pour fournir et produire la Recognised

Environmental Picture (REP), contribuant ainsi à la supériorité de l'information sur le terrain. Le portefeuille des fournisseurs de données géographiques doit comprendre en particulier des cartes et des graphiques normalisés, des informations géographiques essentielles pour la zone de la mission, telle que des fiches pays, des produits spécialisés, tels que des images satellite à haute résolution, des analyses d'évaluation multispectrales et des modèles 3D intuitifs, et des données géographiques numériques pour toutes les armes et tous les systèmes de navigation utilisés dans le cadre de la mission ou par des plateformes opérant dans la zone de la mission (par exemple, les drones). Les produits spécifiques doivent être disponibles dans les heures qui suivent l'alerte ou la demande d'information, puis être complétés par des documents plus détaillés, tels que des cartes à très haute résolution ou des analyses d'images satellite, dans les heures ou les jours qui suivent. La conséquence pour les fournisseurs de services géospatiaux en ce qui concerne le haut débit est la nécessité d'être en mesure de fournir très rapidement, ce qui se traduit par une chaîne de production rapide, peut-être supplémentaire, avec un état de préparation très élevé et la capacité d'intégrer des innovations techniques rapides au sein de l'organisation du fournisseur. Cela nécessite un lien très étroit avec le monde universitaire et la R&D.

Les années 2010 ont marqué un tournant dans le développement de normes dédiées à résoudre les problèmes d'interopérabilités au sein des armées occidentales. Ainsi, le standard GeoPackage, développé depuis 2012, a permis de créer un format ouvert, normalisé, indépendant des plateformes utilisateurs, portable, autodescriptif et compact, utilisable comme base de données géospatiale autonome, comme pour le transfert d'informations géospatiales [366]. Le GeoPackage est fondé sur le SQLite, une bibliothèque en langage C *Open Source* qui implémente un moteur de base de données relationnelles SQL. Ce format permet de résoudre les nombreux problèmes d'interopérabilité en termes de format de données, tout en fournissant un format facile d'utilisation à destination d'un personnel militaire qui n'est pas nécessairement formé à la manipulation de données géographiques. Il se distingue d'autres formats d'échange, comme le fichier Shape développé par Esri, en permettant le transport de l'ensemble des données d'un produit géographique (imagerie vectrice et raster, métadonnée, symbologie) en un seul fichier pouvant s'ouvrir dans n'importe quelle SIG sans nécessiter de convertisseur de données tierces. Le GeoPackage permet de transmettre rapidement tout type d'informations géospatiales, de les visualiser et de les modifier, le tout en supportant un grand nombre de données différentes, vecteur, raster, d'élévation et leurs métadonnées associées en un seul fichier. Développé à l'origine par le corps des ingénieurs de l'armée de Terre américaine (US Army Corp of Engineer), il a également été traduit en profil de norme par l'OGC. La France utilise le format GeoPackage en interne pour l'échange de données géospatiales entre les différents acteurs en charge de

[366] DGIWG, « DGIWG GeoPackage Profile », ST-DP-19-005, 22 septembre 2023.

la production de données géographiques pour les armées depuis de nombreuses années maintenant. Continuellement mis à jour, le GeoPackage en est à sa version 3.1 publiée le 16 novembre 2021, et continue d'incorporer toujours plus de fonctionnalités pour le partage d'informations géospatiales. Cependant, malgré sa facilité d'utilisation, le format GeoPackage ne s'est pas imposé immédiatement.

Aujourd'hui, l'OTAN ne dispose pas encore d'un STANAG normalisant l'utilisation du format GeoPackage. L'idée de développer un standard pour l'utilisation du GeoPackage s'est réellement développée à partir de 2020, et les premiers travaux dans ce sens au DGIWG et à l'OTAN datent de cette période. Cette situation s'explique en grande partie par le quasi-monopole du format Shape développé par la société américaine Esri pour l'échange et le transport des données géographiques en ligne. À ce titre, la publication le 4 octobre 2023 d'un profile DGIWG du GeoPackage est un grand pas en avant pour la diffusion de ce format au sein des armées occidentales, en offrant une norme unifiée répondant aux besoins de la défense à l'ensemble des acteurs du milieu. De plus, ce profil est développé en collaboration avec le bureau de normalisation de l'OTAN. Un des grands avantages du GeoPackage est qu'il est indépendant de tout distributeur privé, là où le format Shape n'est distribué que par la société Esri. Un des risques persistant derrière le maintien du format Shape comme seul format d'échange des données provient de la dépendance de l'ensemble des producteurs de données à un fournisseur privé dont les méthodes commerciales pèsent lourd sur ces mêmes producteurs et dont les stratégies futures sont difficiles à anticiper. De plus, le poids d'Esri sur la scène internationale de la normalisation des données est non négligeable, étant un des participants les plus actifs de l'OGC depuis sa création. Le développement et l'adoption de normes ouvertes, comme le GeoPackage développé par l'OGC, sont un des moyens les plus efficaces de développer l'interopérabilité entre leurs différents systèmes sans être dépendant d'un fournisseur particulier. Le format GeoPackage est particulièrement utile aux acteurs de la défense, puisque le GeoPackage a été conçu en premier lieu pour permettre l'échange de données géospatiales en grande quantité à des utilisateurs évoluant dans des zones disposant d'une faible connexion Internet, voire d'aucune. De plus, cette norme a été portée au DGIWG par le représentant français au sein du Panel n° 5 dédié aux Webservices, démontrant le dynamisme des propositions françaises en matière de normalisation dans le domaine de la défense. Aujourd'hui les développements de la norme GeoPackage au sein du DGIWG s'articulent autour de la création d'un profilé compatible avec les données des programmes de coproduction MGCP/MUVD. Ce développement dénote de nouveau de l'extrême interconnexion des acteurs de la normalisation des données géospatiales au sein de la communauté militaire, en particulier en occident. De plus, un tel développement renforcerait également l'interconnexion, non pas uniquement des nations occidentales déjà présentes au sein de l'OTAN, mais également avec celles qui participent aux programmes de coproduction sans en être membres. Ainsi, le développement de cette norme en matière de partage de

format de donnée a le potentiel de renforcer la coopération entre d'un grand nombre d'armées à l'international tout en facilitant à l'avenir le développement de potentiels futurs programmes de coproduction.

3.3 La révolution GEOINT

La multiplication des types de données disponibles en matière de renseignement, et de capteurs permettant l'acquisition de données géographiques variées (imagerie optique, radar, laser…) et leur combinaison, a mené au début des années 2000 à une mutation de l'emploi de la géographie dans le domaine militaire. Comme le souligne Philippe Boulanger, le *Geospatial Intelligence « apparaît comme une activité spécifique surtout depuis les années 2000 mais ses fondements culturels et techniques se remarquent dès la Première Guerre mondiale »*[367]. Il s'appuie en effet, dans un premier temps, sur l'idée de recoupement d'informations géographiques à partir de sources variées, avant que la révolution numérique ne permette d'en décupler les capacités. Ce sont les États-Unis qui ont saisi en premier les nouvelles possibilités offertes par la combinaison des outils traditionnels du renseignement et des données géographiques en développant le concept de renseignement géographique ou GEOINT (Geospatial Intelligence). Dès 2003, la définition de GEOINT est introduite au sein du code de la loi américaine, le GEOINT étant défini comme *« le terme désignant l'exploitation et l'analyse de l'imagerie et de l'information géospatiale pour décrire, évaluer et représenter visuellement des caractéristiques physiques et des activités géographiquement référencées sur ou autour de la terre. Le renseignement géospatial comprend l'imagerie, le renseignement image et l'information géospatiale »*[368]. Philippe Boulanger précise à cet égard que l'acronyme de GEOINT traduit désormais *« au second abord, la fusion de données géolocalisées multi-sources et multi-capteurs »*[369], dépassant ainsi la seule exploitation de l'imagerie pour englober un processus informationnel global.

Cette définition peut aujourd'hui être étendue à la combinaison de l'ensemble des outils du renseignement, non seulement image (IMINT), mais également humain (HUMINT), source ouverte (OSINT), électromagnétique (ROEM) ou encore de mesure et signatures (MASINT). L'ensemble de ces données est combiné aux informations géospatiales multispectrales, et de plus en plus, accompagné de données issues de la géographie humaine, et analysé par le biais de systèmes d'information géographiques (SIG). Le GEOINT désigne donc avant tout un processus mêlant acquisition de données

---

367 Boulanger Philippe (dir.), *GEOspatial INTelligence : Geoint, un outil géopolitique d'aide à la décision*, Paris, Armand Colin, 2024, Introduction, p. 1.

368 Title 10 U.S. Code §467, https://uscode.house.gov/view.xhtml

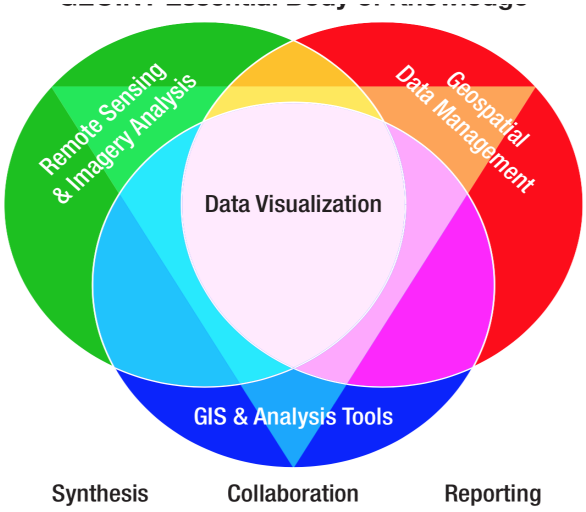
369 Ibid., p. 2.

issues du renseignement, informations géospatiales, puis mise en forme et analyse grâce aux outils SIG, le tout afin de permettre la meilleure visualisation possible des données disponibles sur le théâtre d'opérations (cf. Figure 13). L'expression de *Geospatial Intelligence* s'est surtout développée au sein de la *National Imagery Mapping Agency*, créée en 1996, dont la mission consistait à fusionner les informations liées à l'imagerie, le renseignement image et l'information géospatiale[370]. La mise en application du GEOINT nécessite donc la collaboration des agences de renseignement, de celles en charge de la production de données géospatiales et permet la synthèse des informations disponibles et leur mise en forme afin d'en garantir l'exploitation la plus efficace possible. Au sein de la géographie militaire, le GEOINT est donc l'aboutissement des techniques développées depuis l'époque moderne en termes de description de l'environnement géospatial, soutenues par les dernières avancées technologiques en matière de renseignement et d'acquisition d'information géospatiale. Le tout incorporé au sein d'un processus destiné à maximiser leur exploitation.

Comme le rappelle Gérard Grasse, l'intelligence géospatiale à la française est bien le prolongement de la géographie, car *« c'est sur les bases de la géographie que s'établit le Geoint et qu'il se développe »*[371]. La carte constitue le réceptacle des informations nécessaires à la compréhension d'une situation, et l'apport des SIG facilite la manipulation, le stockage et le partage de ces informations, rendant l'affichage plus agile grâce au changement d'échelles. L'intérêt du GEOINT réside précisément dans sa capacité à intégrer une masse d'informations issues de différents capteurs, favorisant la création de nouveaux supports visuels de l'information et une élaboration plus précise de la représentation cartographique. En ce sens, le GEOINT provoque un changement dans la manière de représenter l'information géographique.

370 Boulanger Philippe (dir.), op. cit., Introduction, p. 3.
371 Grasse Gérard, « Le Geoint : du concept à la doctrine », in Boulanger Philippe (dir.), op. cit., chap. 2, p. 35.

Figure 13 : Représentation de l'ensemble des catégories de savoirs fusionnés dans le cadre du déploiement du GEOINT.



Source : *NewLight Technology (2023)*

Dès 2006, l'armée américaine publie une première version de sa doctrine en matière de GEOINT[372], une première mondiale pour la géographie militaire. Cette doctrine introduit également le concept de Système national pour le renseignement géospatial (*National System for Geospatial Intelligence*, NSG). Ce dernier est décrit comme étant *« la combinaison des technologies, des politiques, des capacités, de la doctrine, des activités, des personnes, des données et des communautés nécessaires pour produire des renseignements géospatiaux dans un environnement intégré, multirenseignement et multidomaine »*[373]. Philippe Boulanger souligne que le GEOINT américain s'inscrit dans le cadre plus large de la *Triade de la puissance militaire* qui repose sur trois composants décisifs, à savoir la conquête spatiale, la triade stratégique nucléaire et l'anticipation stratégique[374]. La mise en place de ce système national souligne bien l'impératif de collaboration multidomaine qui sous-tend la mise en application du GEOINT, et la nécessité de mettre en place une véritable communauté dotée de compétences multiples. Cet écosystème est nécessaire du fait de la grande diversité des données et compétences à mobiliser, qui reste un des grands défis du renseignement géospatial.

---

372 National Geospatial-Intelligence Agency, Office of Geospatial-Intelligence Management, *National System for Geospatial Intelligence : Geospatial Intelligence (GEOINT) Basic Doctrine*, Publication 1-0, septembre 2006.

373 Ibid.

374 Boulanger Philippe (dir.), op. cit., Introduction, p. 4.

En effet, un des nombreux défis à relever lorsque l'on parle de GEOINT tient dans l'incorporation de très nombreuses données différentes, couplées à des informations géospatiales. Les données géospatiales diffèrent des autres données en ce sens qu'elles contiennent des données (emplacement, forme et orientation) relatives aux objets présents à la surface de la terre, ce qui les rend extrêmement volumineuses et encombrantes. Thomas Calix, expert en géographie et en GEOINT au ministère des Armées, précise à cet égard que la discipline du GEOINT consiste à *« produire du renseignement géospatial »*, ce qui suppose de comprendre quelles sont les données dont l'analyste a besoin pour répondre à une problématique dans un contexte défini dans le temps et dans l'espace[375]. Les données géospatiales proviennent de divers capteurs et sources, et dans une variété de formats qui augmentent le risque d'incohérences. La normalisation des données est donc un facteur capital pour permettre le déploiement du processus propre au GEOINT, qui nécessite d'incorporer l'ensemble de ces données au sein de multiples systèmes d'information et systèmes d'armes employés par les forces armées. La fourniture d'informations géospatiales opportunes, précises et pertinentes est un outil essentiel tout au long du processus opérationnel pour développer une connaissance partagée de la situation, améliorer la compréhension des capacités et des limites des forces amies et ennemies, et mettre en évidence d'autres conditions de l'environnement opérationnel pour les forces engagées sur le terrain[376]. La question de la gouvernance des données revêt dans ce cadre une importance particulière. Comme le démontre Éric Tribain, *« la donnée est devenue un enjeu majeur devant son accroissement et sa capacité à fournir de la connaissance »* [377], ce qui impose de l'intégrer dans une stratégie de gouvernance rigoureuse pour assurer la cohérence de l'activité GEOINT.

Conscient du problème capital que constitue la normalisation des données pour la mise en application du GEOINT, l'armée américaine a créé un centre au sein du NSG dédié aux standards du GEOINT, le *National Center for Geospatial Intelligence Standard* (NCGIS)[378]. La création de ce centre souligne la prise de conscience de l'importance des normes géospatiales, dont seule l'adoption peut garantir la livraison de données géospatiales de qualité, et suffisamment rapidement pour répondre aux exigences de professionnels de la défense. De plus, l'adoption de normes internationales est nécessaire dans le cadre de déploiement en coalition, ces dernières réduisant les coûts et le temps de production des données. Ainsi, l'interopérabilité est une pierre angulaire de la production géospatiale.

---

375 Calix Thomas, « Les capteurs et systèmes d'acquisition du Geoint », in Boulanger Philippe (dir.), op. cit., chap. 3, p. 55.

376 U.S. Army, *Techniques Publication No. 3-34.80 « Geospatial Engineering »*, Headquarters Department of the Army, Washington, DC, 22 février 2017.

377 Tribain Éric, « La gouvernance, système et données », in Boulanger Philippe (dir.), op. cit., chap. 4, p. 75.

378 National Geospatial-Intelligence Agency, « Geospatial Intelligence Standard. Enabling a Common Vision », novembre 2006.

Afin de relever le défi de l'interopérabilité, les États-Unis s'appuient sur l'ensemble des organismes internationaux de normalisation de données géospatiales, à la fois civils et militaires, au sein desquels ils sont systématiquement présents afin de constituer un ensemble de standards interconnectés, nécessaires à la création d'une architecture orientée services dédiée aux membres de la communauté GEOINT au sein de leurs forces armées. Cet effort international sans équivalent dans le monde rassemble différentes organisations diversement impliquées dans ce processus, liant dans une toile complexe un vaste ensemble de pays plus ou moins étroitement liés aux États-Unis. Philippe Boulanger rappelle que le GEOINT américain constitue un *« fondement de toute puissance globale »* en raison de sa supériorité informationnelle, et que de nombreux autres États et organisations internationales se sont dotés de capacités de fusion depuis les années 2010[379]. Ainsi, si les organisations internationales, comme l'ISO TC/211 et l'OGC fournissent les normes abstraites qui composent les fondations de cette architecture normative, ce sont d'autres organismes plus spécialisés, et qui rassemblent un ensemble précis de pays tels que le DGIWG, qui développent la majorité des normes formant les blocs d'assemblage de cette architecture GEOINT internationale. Cet ensemble d'acteurs et d'organisations diverses compose ainsi une toile complexe d'interaction civile et militaire à l'échelle internationale au sein de laquelle la France joue un rôle important.

Les normes géospatiales en soutien du GEOINT sont ainsi développées aux côtés des autres normes en matière de production de données géographiques, généralement par des organismes spécialisés, tels que le DGIWG ou l'OTAN. À ce titre il n'est pas anodin que les membres américains du P5 au sein du DGIWG soient membres du NCGIS. Parmi les récents développements en matière de normes GEOINT, on peut citer, outre la norme EDR[380] développée par le Panel 5 du DGIWG citée précédemment, le projet du MASINT *Working Group* de la NGA présenté au DGIWG en octobre 2023. Le but de ce projet est d'arriver à produire un profil DGIWG de solutions normatives permettant le partage d'informations provenant d'outils de capture de mesure et signatures entre différents systèmes de renseignement dans un environnement fondé sur le Web pour les applications de renseignement, de surveillance et de reconnaissance. Cet ensemble de normes devra permettre une représentation numérique cohérente et homogène des observations provenant de données et de types de capteurs variés. Ce projet en est encore à ses balbutiements et seule une note d'intention de la part du MASINT *Working Group* de la NGA existe à l'heure actuelle. Cependant il est certain que le travail de normalisation dans ce domaine sera poursuivi en collaboration avec le Panel 5 du DGIWG au vu des

379 Boulanger Philippe (dir.), op. cit., Introduction, p. 5-6.

380 Environnement data retrieval (EDR) : une API de récupération de données environnementales fournit une interface de programmation d'application pour accéder aux ressources de données environnementales et météorologiques.

avantages certains pour les armées que procurerait une architecture normative homogène pour le partage d'informations issues de capteurs de mesure et signatures.

Un autre projet tourné vers le soutien GEOINT en matière de norme tient au développement d'une nouvelle génération de normes concernant l'imagerie de renseignement, de surveillance et de reconnaissance (*Intelligence, Surveillance, Reconnaissance Imagery*, ISR), la norme NGIIS (*Next Generation ISR Imagery Standard*). Soutenu par la *GEOINT and IT Standard Division* de la NGA et l'OTAN, le but est de développer de nouvelles normes pour la communauté militaire en matière d'imagerie ISR. Le projet soutenu par la NGA cherche avant tout à tirer parti de l'industrie commerciale de diffusion en continu (*streaming*), qui représente déjà plusieurs milliards de dollars, pour fournir des images GEOINT aux ministères de la Défense des pays de l'Alliance atlantique au moment et à l'endroit où elles sont nécessaires. Cet ensemble de normes se devra d'être fondé sur des normes ouvertes déjà utilisées par l'industrie, mais calibrées pour les besoins de la défense. Ces normes prendront en compte à la fois les images fixes, multispectrales et hyperspectrales, et les images animées provenant, par exemple de drones. Elles devront également être indépendantes de tout matériel informatique propriétaire, compatibles avec les technologies cloud et permettre le traitement des images par l'intelligence artificielle et le *machine-learning*. Aujourd'hui, le format privilégié au sein de la communauté de la défense pour le transfert de données images est le format NITF (*National Imagery Transmission Format*) développé par Esri. L'avantage du développement de la norme NGIIS est de s'émanciper d'un format de fichier propriétaire rigide et non compatible avec les technologies du cloud, pour se diriger vers une nouvelle norme open source et plus flexible en termes de modes de transfert. Ce travail est poursuivi en parallèle au sein de l'ISO avec le développement de la norme ISO/IEC 23001-17[381] sur un nouveau format de fichier pour le transfert de données vidéos et audios non compressés. Le cas du NGIIS est un bon exemple de l'extrême interconnexion des diverses organisations de normalisation en matière de normes géographiques, et de la collaboration des diverses instances de normalisation dans un même domaine technique.

Toujours est-il que le GEOINT, en mobilisant un grand nombre de domaines techniques pour aboutir à une fusion de données toujours plus nombreuses et efficaces, nécessite le développement d'un grand nombre de normes à la fois dans le domaine des sciences géographiques, mais également dans celui des technologies de l'information et de la communication au sens large. Thomas Calix, dans sa contribution consacrée au GEOINT dans les opérations militaires, souligne que celui-ci « contribue par la fusion des renseignements à l'évaluation rapide de l'environnement », ce qui suppose une

[381] ISO/IEC, « FDIS 23001-17. Information technology. MPEG system technologies. Part 17 : Carriage of uncompressed video and images in ISO Base Media File Format » (en développement).

appréciation contextualisée par les informations géographiques GHOM, c'est-à-dire géographique, hydrographique, océanographique et météorologique[382]. De nombreux projets en développement au sein du DGIWG, mais également de l'ISO et de l'OGC sont tournés vers l'intégration de données dont le développement renforcera les capacités GEOINT de toutes les nations qui prennent part à leur développement, et qui seront les premières à pouvoir en tirer profit une fois ces normes publiées et intégrées à leur chaîne de commandement militaire.

Comme indiqué précédemment, la France est un des rares pays capables de produire en autonomie l'ensemble de ses informations géospatiales, en s'appuyant sur un tissu industriel robuste, et des technologies de pointe dans le domaine spatial. Il faut attendre 2013 pour voir le terme de GEOINT apparaître dans un rapport à l'Assemblée nationale par les députés Patrice Verchère et Jean-Jacques Urvoas concernant l'évaluation du cadre juridique applicable aux services de renseignement[383]. La place centrale du GEOINT au sein de l'infrastructure militaire française est confirmée par la création du Centre de renseignement géographique interarmées (CRGI) en 2015. Philippe Boulanger note à cet égard que « le ministère des Armées crée un premier centre Geoint en 2014 tandis que sa première doctrine est adoptée en juillet 2021 »[384], confirmant ainsi l'intégration progressive du GEOINT dans l'appareil de défense national.

L'organisation française du GEOINT se distingue du modèle américain par une architecture institutionnelle spécifique, structurée autour de plusieurs acteurs complémentaires. Au cœur du dispositif, la Direction du renseignement militaire (DRM), créée en 1992, constitue l'acteur central du renseignement militaire français et le principal exploitant des capacités GEOINT au niveau interarmées[385]. C'est au sein de la DRM que s'opère la fusion des renseignements d'origine géospatiale avec les autres sources de renseignement, conformément au processus décrit plus haut. La Direction générale de la sécurité extérieure (DGSE) dispose également de ses propres capacités d'exploitation géospatiale, qu'elle mobilise dans le cadre de ses missions de renseignement extérieur. La DGSE exploite notamment l'imagerie satellitaire à des fins de renseignement stratégique, en s'appuyant sur les capacités du programme d'observation spatiale militaire français CSO (Composante Spatiale Optique), dont les satellites fournissent de l'imagerie à très haute résolution[386]. Cette imagerie est

382 Calix Thomas, « Le Geoint et les opérations militaires », in Boulanger Philippe (dir.), op. cit., chap. 7, p. 139.

383 Urvoas Jean-Jacques et Verchère Patrice, « Rapport d'information par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement », Assemblée nationale, n° 1022, 14 mai 2013.

384 Boulanger Philippe (dir.), op. cit., Introduction, p. 7.

385 Sur la DRM et son rôle dans le renseignement géospatial, voir : Ministère des Armées, « La Direction du renseignement militaire », 2023. La DRM a été créée par le décret n° 92-523 du 16 juin 1992 portant création de la Direction du renseignement militaire.

386 Sur le programme CSO et ses capacités, voir : Ministère des Armées, « Les capacités spatiales militaires », 2023. Le programme CSO, qui a succédé aux satellites Helios, comprend trois satellites fournissant de l'imagerie optique à très

exploitée tant par la DRM que par la DGSE, en coordination étroite lorsque les théâtres d'opérations l'exigent. Ce dualisme entre renseignement militaire et renseignement extérieur constitue une spécificité française qui, si elle peut complexifier la chaîne de commandement, permet également une couverture plus large du spectre du renseignement géospatial.

Du côté de la production de données, l'Institut national de l'information géographique et forestière (IGN), à travers son homologue militaire incarné historiquement par le Bureau géographie, hydrographie, océanographie et météorologie (BGHOM) (aujourd'hui section Géo) et le service géographique des armées, assure la production, la gestion et la diffusion de l'information géospatiale nécessaire aux forces armées. Le rôle de l'IGN dans le dispositif GEOINT français est fondamental dans la mesure où il fournit les référentiels géographiques de base, qu'il s'agisse des données topographiques, des modèles numériques de terrain ou encore de l'ortho-imagerie, sur lesquels viennent se superposer les couches de renseignement exploitées par la DRM. Le 28e groupe géographique, unité opérationnelle de l'armée de terre déployée sur les théâtres d'opérations, complète ce dispositif en assurant la production cartographique de terrain et l'acquisition de données géospatiales au plus près des forces engagées. Cette organisation tripartite, fondée sur la DRM pour l'exploitation et la fusion, l'IGN et le BGHOM pour la production des référentiels, et le 28e groupe géographique pour l'acquisition opérationnelle, forme l'ossature du GEOINT à la française[387]. Ce modèle, s'il est plus modeste en moyens que le système américain, n'en demeure pas moins l'un des plus complets en Europe.

Depuis la création du CRGI, l'importance du GEOINT n'a cessé de progresser au sein des institutions nationales. Ainsi, en 2020, le ministère de l'Intérieur a inscrit le GEOINT dans son dernier livre blanc en soulignant le besoin de renforcer l'emploi de la géographie numérique comme outil d'aide à la décision[388]. La Loi de programmation militaire 2024-2030 confirme cette dynamique en consacrant une enveloppe significative au renseignement et au numérique, témoignant de l'importance stratégique accordée par l'État français à la maîtrise de l'information géospatiale[389].

La place de la France est unique au sein de cet écosystème international de production de normes géospatiales dédiées au domaine militaire. Sa position de leader dans le domaine de la normalisation internationale civile, tant au sein de l'ISO/TC 211 que du CEN/CENELEC, en fait un

haute résolution.

387 Sur la structuration du GEOINT français et la comparaison avec les modèles étrangers, voir Boulanger Philippe (dir.), op. cit., chapitres 8 à 10, consacrés respectivement aux modèles britannique, européen et aux perspectives internationales.

388 Ministère de l'Intérieur, *Livre blanc de la sécurité intérieure*, 2020, p. 233.

389 Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030. La LPM prévoit une enveloppe de 20 milliards d'euros consacrée au numérique.

acteur incontournable de cet ensemble. Cependant, son influence et sa capacité financière ne rivalisent pas pour autant avec celles des États-Unis, qui fédèrent la majorité des acteurs du milieu militaire dans lequel évolue la France, que ce soit au niveau de l'OTAN ou plus généralement sur la scène internationale, de par leur poids diplomatique et militaire. De plus, nombreux sont les pays à avoir noué avec les États-Unis des relations particulières, comme les membres des *Five Eyes*, accord de partage qui rassemble les agences de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis[390], ce qui n'est pas le cas de la France. La balance entre ses propres intérêts et son allié américain est donc plus délicate pour la France, qui dispose de ses propres programmes en matière de GEOINT, comme le programme GEODE 4D, et d'impératifs militaires parfois très particuliers du fait des nombreux déploiements étrangers des armées françaises. Cependant, malgré ces particularités, la France reste très intégrée à l'ensemble des programmes et institutions qui développent des normes géospatiales, qu'il s'agisse de l'OTAN, du DGIWG ou encore des programmes de coproduction militaire auxquels elle participe.

Ainsi, aucune donnée géographique n'est produite aujourd'hui au sein des armées qui ne soit conforme aux normes internationales adoptées, qu'il s'agisse de celles de l'OTAN, du DGIWG et des spécifications des programmes de coproduction quand cela s'applique. La dimension internationale de cette production est entièrement intégrée au processus de production de ces données, en application des impératifs imposés par les déploiements en coalition de l'armée française, ces besoins se surimposant aux besoins particuliers des opérationnels. La seule exception à cette règle tient aux productions cartographiques *ad hoc* créées par les soldats du 28e groupe géographique déployés sur les théâtres d'opérations, lorsqu'aucune autre donnée ne peut satisfaire les besoins de la mission. La stratégie française en matière de production de données est dictée avant tout par la stratégie établie dans le dernier livre blanc sur la défense nationale de 2013. Le renseignement géographique répond en particulier à la fonction de connaissance et d'anticipation, qui recouvre notamment le renseignement et la prospective, qui « permet l'anticipation stratégique et qui éclaire l'action »[391]. Concrètement cela se traduit pour le BGHOM par la nécessité de garantir une production et un approvisionnement suffisant en information géospatiale pour les hommes, les systèmes d'armes et les systèmes d'information à la hauteur des ambitions du Livre blanc. Le choix de renforcer les partenariats internationaux pour la production de données géospatiales, tout en s'appuyant sur des partenariats industriels, a été fait afin de répondre à cet objectif, dans un contexte de diminution des effectifs et d'expansion des zones de déploiement.

---

390 Five Eyes Intelligence Oversight and Review Council, « Charter of the Five Eyes Intelligence Oversight and Review Council », 2 octobre 2017.

391 Direction de l'information légale et administrative, *Livre blanc Défense et Sécurité nationale*, 2013, p. 70.

Conclusion du chapitre III

Comme cela a été démontré dans ce chapitre, l'écosystème international de la normalisation des données géographiques repose sur un équilibre complexe entre organismes internationaux, consortiums privés et instances européennes. L'ISO et l'IHO jouent un rôle fondamental dans l'établissement de standards reconnus à l'échelle mondiale, garantissant une interopérabilité essentielle entre les acteurs du secteur. La gouvernance et la structure décisionnelle de l'ISO, bien que marquées par une domination historique des pays occidentaux, restent le théâtre d'une compétition stratégique où émergent de nouveaux acteurs, notamment asiatiques, à l'image de la Chine et de la Corée du Sud. Parallèlement, les consortiums privés, tels que l'Open Geospatial Consortium (OGC) et le World Wide Web Consortium (W3C) viennent compléter ce paysage en favorisant le développement de normes techniques directement influencées par les besoins industriels et commerciaux. Ces entités, soutenues par des géants technologiques, jouent un rôle clé dans l'innovation et l'adoption rapide de standards en adéquation avec les avancées du marché. Leur interaction avec les instances normatives publiques permet d'assurer une convergence entre innovation technologique et cadre réglementaire. La France, bien qu'influente au sein des organismes internationaux de normalisation, doit maintenir son engagement stratégique pour préserver son leadership face à des dynamiques géopolitiques en mutation. La montée en puissance de la Chine, ainsi que le retrait progressif des États-Unis de certaines instances, redessine progressivement les équilibres en matière de gouvernance normative. Ainsi, la normalisation des données géographiques constitue un enjeu stratégique de premier ordre, impactant non seulement les industries et les administrations publiques, mais aussi la souveraineté numérique et l'interopérabilité mondiale. La capacité des acteurs à s'impliquer dans ces instances demeure un levier essentiel pour influencer l'orientation des standards et garantir leur alignement avec les intérêts nationaux et régionaux.

Au sein de cet écosystème international, l'Union européenne joue un rôle central. Grâce aux institutions telles que le CEN, le CENELEC et l'ETSI, ainsi qu'à l'adoption de la directive INSPIRE, l'Europe a su imposer une gouvernance efficace en matière de normalisation des données géographiques, garantissant une uniformisation des standards tout en renforçant la compétitivité de son industrie sur la scène internationale. La France, en tant qu'acteur majeur de la normalisation européenne, bénéficie d'une influence significative, notamment grâce à son implication au sein des instances de gouvernance et de coordination. Son leadership, illustré par sa forte représentation au sein des comités techniques et son rôle clé dans l'adoption des normes européennes, lui permet de défendre ses intérêts tout en contribuant à la consolidation d'un espace normatif cohérent et intégré. Toutefois,

malgré ces avancées, des défis demeurent. L'interopérabilité effective des jeux de données, la mise en œuvre harmonisée de la directive INSPIRE à travers les États membres, et la nécessité de mieux coordonner les différentes initiatives européennes reste un enjeu majeur. De plus, la concurrence internationale, notamment face aux États-Unis et à la Chine, impose à l'Europe de renforcer sa stratégie pour garantir la souveraineté et la pérennité de ses normes. Dans ce contexte, la normalisation des données géographiques représente bien plus qu'un simple enjeu technique. Elle constitue un levier stratégique, aussi bien pour la protection de l'environnement et la gestion des territoires que pour le développement économique et la défense. L'Union européenne doit ainsi poursuivre ses efforts pour affirmer son indépendance et anticiper les évolutions technologiques, tout en veillant à préserver l'indépendance et la compétitivité de ses industries. Ainsi, la normalisation des données géographiques est un enjeu stratégique fondamental pour les armées modernes, tant sur le plan national qu'international. L'évolution des outils numériques, le développement du GEOINT et l'accélération des échanges d'informations géospatiales ont transformé la manière dont les forces armées perçoivent et exploitent leur environnement. La France, forte de son expertise dans la production de données géographiques, bénéficie d'une autonomie remarquable dans ce domaine, grâce à son tissu industriel et à ses partenariats avec des acteurs publics tels que l'IGN. Cependant, l'interopérabilité reste un défi majeur dans un contexte où les interventions en coalition se multiplient et où les standards internationaux évoluent en permanence. L'intégration des normes OTAN, DGIWG et des spécifications des programmes de coproduction permet de garantir une compatibilité optimale des données géographiques militaires entre alliés. Cependant, la nécessité de concilier les exigences nationales avec celles d'une architecture normative internationale impose des arbitrages constants, notamment vis-à-vis de la prépondérance américaine dans ce domaine. L'adoption progressive de formats ouverts, comme le GeoPackage illustre la volonté des acteurs militaires de s'affranchir de certaines dépendances technologiques et d'assurer une meilleure flexibilité opérationnelle. Enfin, l'essor du GEOINT marque une révolution dans l'exploitation des données géographiques en intégrant des sources variées issues du renseignement et en mobilisant des technologies avancées, comme l'intelligence artificielle. La France, bien qu'intégrée dans les grands projets internationaux, doit continuer à investir dans ce domaine afin de maintenir son autonomie stratégique et de répondre aux exigences croissantes de la guerre moderne. L'adoption de nouvelles normes et la coopération renforcée avec les organismes civils et militaires resteront des leviers essentiels pour garantir la supériorité informationnelle et opérationnelle des forces armées françaises.

Conclusion de la partie 1

Ainsi, la normalisation des données géographiques numériques tant dans le domaine civil que militaire s'inscrit bien dans le cadre de la compétition internationale à la fois dans le domaine de la normalisation et de la cybersécurité. Outil essentiel de l'État moderne dans l'affirmation de sa souveraineté, les données géographiques constituent une ressource d'une importance capitale dont la maîtrise et la diffusion sont un enjeu de premier plan pour l'État. Alors que le numérique constitue le mode de production et de diffusion qui privilégie des données géographiques, la cybersécurité devient également un enjeu majeur dans la préservation et la conception de ces données. La compétition internationale en matière de normalisation se déploie à différentes échelles territoriales qui mêlent différents acteurs de nature très différents, impliqués dans ces luttes de pouvoir pour façonner l'orientation des technologies futures concernant les données géographiques. Ainsi, la compétition en matière de normalisation a des conséquences sur les modalités de production de ces données géographiques et par extension sur les conditions d'emploi de ces dernières, obligeant les États à se pencher sur cette compétition afin de préserver leur maîtrise de cet outil essentiel à leur souveraineté qui ne peut être laissé entièrement entre les mains des sociétés privées. L'État français est largement impliqué dans ces mécaniques et occupe une place privilégiée sur la scène internationale tant dans le domaine civil que militaire. Cependant cette position ne doit pas faire oublier les efforts nécessaires à la préservation voir à l'amélioration de cette position. Le retour en force de la Chine sur la scène internationale dans le domaine de la normalisation, ainsi que les impératifs de la production géographique militaire, qui repose sur ses propres circuits de normalisation en étroite collaboration avec ses alliés, est un constant rappel de l'importance cruciale de ces processus normatifs pour la France. La stratégie française en matière de normalisation des données géographiques doit rester globale et assurer à la fois la mise en valeur de son expertise sur la scène internationale tout en participant à maximiser l'usage des données géographiques à l'échelle nationale ainsi que la protection contre les menaces cyber qui apparaissent aujourd'hui comme une nouvelle menace encore sous-estimée par les acteurs de la production des données géographiques.

Partie 2 - Risque cyber et normalisation des données géographiques

Alors que les données géographiques numériques sont de plus en plus exposées aux menaces cyber, dans quelle mesure les normes techniques existantes permettent-elles d'en assurer la protection, face à l'émergence d'un cyberespace structuré par des rapports de force géopolitiques croissants ? Dans cette seconde partie, vont être explorés en profondeur les défis liés à la sécurité des données géographiques face aux cyberattaques. Dans un premier temps sera abordée la question des défis propres à la protection de ces données à l'ère numérique. En effet, la protection de ces données relève d'enjeux de souveraineté, en particulier pour les États, et faillir à cette protection peut avoir de graves conséquences. Les efforts en matière de normalisation de ces données participent à renforcer la résilience des infrastructures de données géographiques en ligne. Dans une deuxième partie, nous nous concentrerons sur la nécessité de la protection des plateformes de données géographiques, qui sont aujourd'hui les principaux outils de diffusion de ces données, et qui sont désormais au cœur des attaques lancées par les pirates informatiques. De même, ces questions restent cruciales concernant les architectures réseau employées par les forces armées. Nous verrons aussi quelles mesures ont été prises pour garantir la protection des réseaux militaires en charge de la gestion et de la diffusion des données géographiques. Enfin, dans une troisième partie, la protection des infrastructures de mise à disposition des données géographiques dans les territoires, qui présentent aujourd'hui une grande disparité concernant la prise en compte de ces menaces et leur capacité à y faire face, sera étudiée. De plus, les rapports entre ces mêmes collectivités et l'État concernant la gestion de ces données et les politiques en matière de normalisation qui sont appliquées nécessitent également d'être développée. Enfin, la dernière partie s'attardera sur une étude de cas concernant le nouveau projet de jumeau numérique des territoires et la manière dont ce dernier cristallise les risques et les enjeux concernant la protection et la diffusion des informations géographiques.

Chapitre IV- Les enjeux de la protection des données géographiques contre le risque cyber

1. Protéger les données géographiques à l'ère de la numérisation

1.1 Les données géographiques : des données toujours plus vulnérables aux attaques informatiques

Comme souligné dans le premier chapitre, la cybersécurité est aujourd'hui un enjeu majeur pour l'ensemble des utilisateurs et producteur de données géographiques en ligne. Le cyberespace constitue aujourd'hui l'espace de diffusion privilégié des données géographiques, nécessitant de développer des capacités de protection adéquate de ces données. La cybersécurité est un défi mondial, car le cyberespace n'est jamais sans risque. La cybersécurité garantit l'obtention et le maintien des propriétés de sécurité de l'infrastructure et des services numériques contre les risques de sécurité liés au cyberespace. La cybersécurité est un ensemble d'outils, de politiques, de concepts de sécurité, de garanties de sécurité, de lignes directrices, d'approches de gestion des risques, d'actions, de formations, de bonnes pratiques, d'assurance et de technologies qui peuvent être utilisés pour protéger le l'environnement cyber d'une organisation et/ou d'un individu[392].

Les données géographiques présentent des défis uniques en matière de cybersécurité, non seulement parce qu'elles sont souvent associées à des questions de souveraineté, mais aussi parce que de nombreuses infrastructures de données comprennent des données cartographiques sensibles, ainsi que de nombreuses données environnementales et urbaines précieuses générées à des fins de gestion, de planification et de prévision. Compromettre l'intégrité d'une base de données géographiques peut avoir de graves conséquences, car celles-ci jouent souvent un rôle essentiel dans de nombreux processus de prise de décision aux niveaux régional et national, notamment en matière d'urbanisme, de gestion des catastrophes naturelles, d'affectation des ressources et de navigation maritime, pour ne citer que quelques exemples. De plus, la composante multidimensionnelle des bases de données géographiques (à savoir, un large éventail de couches de données) conduit à la création de systèmes complexes particuliers qui sont sujets à un large éventail de menaces possibles, et dont l'identification est loin d'être aisée. Cela fait des bases de données géographiques et de leurs infrastructures des systèmes particulièrement sensibles à sécuriser contre les cyberattaques et les fuites.

Depuis longtemps, des efforts en matière de normalisation ont été déployés dans le domaine des systèmes d'information géographique (SIG) afin de promouvoir l'interopérabilité, le partage des

[392] R. Von Solms, et J. Van Niekerk, « From information security to cyber security. », Computers & security, n° 38, pp. 97-102, 2013.

données et la sécurité. Ces normes visent à renforcer la résilience des SIG et à atténuer les risques de cyberattaques. Ainsi, les normes ISO jouent un rôle important dans le renforcement de la cybersécurité et fournissent des lignes directrices aux organisations pour qu'elles mettent en place des pratiques de sécurité robustes. Les efforts de normalisation, comme le développement des normes ISO contribuent de manière significative à l'amélioration de la sécurité des infrastructures de données SIG. Cependant, elles ne peuvent pas garantir une protection totale contre toutes les cyberattaques. La série de normes ISO 19100 est spécifiquement orientée vers l'interopérabilité des bases de données géographiques. En ce qui concerne la diffusion et la dissémination à grande échelle des données géographiques, les services web jouent un rôle majeur. En particulier, l'Open Geospatial Consortium (OGC) a publié plusieurs normes qui permettent aux services web d'échanger, d'accéder et d'intégrer des données géographiques sur différentes plateformes et systèmes. Les normes les plus courantes sont le Web Map Service (WMS) pour la représentation, le Web Feature Service pour le téléchargement et le Web Catalog Service pour la découverte de données géographiques[393] (cf. Figure 14) .

Toutes ces normes impliquent la manipulation des données vecteurs et à la sémantique associée, et requièrent des mécanismes spécifiques de protection des données, car leur diffusion auprès de vastes communautés d'utilisateurs accroît le risque de menaces ainsi que leur impact potentiel. Une autre particularité de ces normes réside dans le fait que nombre d'entre elles sont interdépendantes, comme la famille de normes S-100 mise en œuvre pour la nouvelle génération de cartes de navigation. Par ailleurs, la norme S-100 intègre étroitement les normes de l'OGC pour la diffusion en temps réel à l'aide de services web.

Ce problème n'est pas spécifique au domaine géographique, mais en réalité courant, comme en témoigne les séries de vulnérabilités signalées dans d'autres normes, comme le protocole ISO 15118 (interface de communication véhicule réseau)[394]. Une réponse intéressante à ces problèmes consiste à traiter les risques de cybersécurité dès la conception des normes. Les normes étant susceptibles de fonctionner à grande échelle et d'être largement diffusées, toute vulnérabilité peut potentiellement avoir de nombreuses répercussions en cascade. Dans le contexte des normes d'information géographique, l'éventail des utilisateurs potentiels étant très large, toute vulnérabilité des services web mis en œuvre pour la diffusion des données géographiques est susceptible d'avoir un impact dévastateur. En outre, les normes géographiques sont largement interconnectées, en raison du large éventail de sources de données impliquées provenant de phénomènes physiques, environnementaux et humains. Par

[393] Kelvin Lawrence, Kaler Chris, Nadalin Anthony, Monzillo R, et Hallam-Baker P, « Web services security : Soap message security 1.1 (ws-security 2004) », *OASIS, OASIS Standard*, Février 2006.

[394] Kaibin Bao, Hristo Valev, Wagner Manuela, et Hartmut Schmeck, « A threat analysis of the vehicle-to-grid charging protocol iso 15118 », Computer Science-Research and Development, 33, 2018, pp. 3 – 12. ; Köhler Sebastian, Baker Richard, Strohmeier Martin, et Martinovic Ivan, « Brokenwire : Wireless disruption of ccs electric vehicle charging », 2022.

conséquent, toute vulnérabilité d'une norme est susceptible d'avoir un impact important, ce qui constitue une motivation majeure pour identifier clairement les interdépendances entre les différentes normes, leur sécurité respective et les conséquences possibles de toute menace cybernétique et de toute vulnérabilité. Dans l'ensemble, la sécurisation d'un ensemble de normes interdépendantes est un problème majeur à traiter et à résoudre.

Ainsi, les données géographiques en ligne peuvent constituer des cibles de choix pour les pirates informatiques. Afin de mieux cerner les risques qui entourent les données géographiques numériques, il est essentiel de comprendre comment peuvent se manifester ces attaques sur des architectures de données géographiques en ligne.

1.2 : Les principes de sécurité informatique appliqués aux données géographiques : comprendre le traitement des données géographiques en ligne

La sécurité des données repose sur quatre principes : l'intégrité, la confidentialité, la disponibilité et le respect de la vie privée, qui sont essentiels pour protéger les données sensibles contre diverses menaces, telles que l'accès non autorisé, les fuites de données et la manipulation. Dans le domaine géographique, sont considérées comme sensibles les données dont la compromission pourrait porter atteinte à la sécurité nationale (infrastructures critiques, installations de défense), à l'exercice des droits des personnes (données cadastrales, plans de prévention des risques), aux intérêts économiques des acteurs (données de planification, ressources naturelles) ou à la vie privée des individus (données de géolocalisation). L'intégrité est liée à l'exactitude et à la fiabilité des données tout au long de leur cycle de vie et doit garantir la protection des données contre la suppression, la modification ou les fausses injections non autorisées ou non détectées. La confidentialité des données est la capacité de stocker des données sensibles et d'en restreindre l'accès à l'aide de processus de contrôle, d'authentification et de chiffrement[395]. La disponibilité des données est la capacité de fournir les bonnes données à tout moment, sans compromis, même en cas d'incident, tel que l'endommagement du disque dur, l'incendie des serveurs et les pannes de réseau[396]. La confidentialité des données est définie comme « la capacité d'un utilisateur ou d'un groupe d'utilisateurs à s'isoler ou à isoler des informations le concernant et à les révéler de manière sélective »[397].

---

395 Kosinski Matthew, et Forrest Amber, « Qu'est-ce que la confidentialité des données ? », IBM, 19 décembre 2023. https://www.ibm.com/fr-fr/topics/data-privacy?

396 Vachot Isora, « Intégrité, Confidentialité, Disponibilité : définitions », Cybersecura, 26 avril 2024. https://www.cybersecura.com/post/integrite-confidentialite-disponibilite-definitions-1?

397 Vigouroux Gauthier, Merino Laso Pedro, Claramunt Christophe, et Leidinger Nathalie, « Evaluating the vulnerability of iso 19100 and s-100 standards through visual approaches ». In *Proceedings of the 30th International Conference on Advances in Geographic Information Systems*, pp.1–4, 2022.

Parmi les nombreux domaines où les principes de sécurité des données ont été appliqués, les services de localisation et la fourniture de services de cartographie sont des domaines importants et sensibles où les violations de la sécurité pourraient avoir un impact significatif. Ces services reposent en grande partie sur des données géographiques, généralement matérialisées par une série de couches thématiques de préférence structurées, comme des objets spatiaux (c'est-à-dire des points, des polylignes et des régions)[398]. En raison de leur composante spatiale et de leurs propriétés spécifiques, les données géographiques ont des exigences particulières en matière de sécurité, telles que la protection des données, la confidentialité, l'intégrité, la gestion des privilèges d'accès, la protection des droits d'auteur, la non-répudiation et la disponibilité [399]. Les questions de sécurité, lorsqu'elles sont appliquées au domaine des données géographiques, ont des exigences spécifiques liées à la nature multidimensionnelle et à la complexité des données géographiques, aux très grandes bases de données généralement générées ainsi qu'à leur importance pour de nombreuses questions juridiques associées à leur utilisation[400].

L'émergence d'internet a largement réduit les coûts liés à la gestion de données et à la diffusion massive d'informations. Ces derniers se sont développés dans le monde entier, au même titre que leurs nombreux domaines d'usages[401]. Le domaine des SIG en ligne a évolué très rapidement, de par leur utilité grandissante en tant que services accessibles en ligne, et à l'évolution fulgurante et parallèle des technologies numériques et des SIG[402]. Les SIG en ligne ont rendu accessibles à n'importe qui les informations géographiques, et ont très largement élargies leurs usages, en transformant les données géographiques brutes en services géographiques standardisés à travers le développement d'applications, comme celles dédiées aux voyages (Google Maps, Waze), aux services des secours, au tourisme, à la gestion des ressources naturelles, etc…[403]

En 2025, la diffusion ou la dissémination des données géographiques est généralement facilitée par divers services web (Web Service : WS). Les services web sont une composante essentielle du développement web moderne, permettant à différentes applications et systèmes de communiquer et

---

398 Samet Hanan., « Spatial data structures »., 1995.

399 Hanashima Makoto, « Consideration for information security issues in geospatial information services of local governments ». IASSIST Quarterly, n°29, 2006. ;
Solymosi Reka, Buil-Gil David, Ceccato Vania, Kim Eon, et Jansson Ulf, « Privacy challenges in geodata and open data »., Area, n/a(n/a).

400 Bertino Elisa, Thuraisingham Bhavani, Gertz Michael, et Damiani Maria Luisa, « Security and privacy for geospatial data », *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*, novembre 2008.

401 Ozturan, M., Egeli, B., et F. Bacioglu., « Web-GIS based urban management information system: the case of satellite cities in Istanbul », Management Information Systems, 2004 : GIS and Remote Sensing, n°8, pp.13-21, 2004.

402 Liu, X., Han, J., Zhong, Y., Han, C., He X., « Implementing WebGIS on hadoop: A case study of improving small file i/o performance on HDFS. », IEEE international conference on cluster computing and workshops, Cluster' 09, pp. 1–8, 2009.

403 Agrawal, S. et Gupta, R. D., « Web GIS and its architecture: a review. », Arabian Journal of Geosciences, 10, 518, 2017.

d'échanger des données sur l'internet. Les services web reposent sur des protocoles et des formats de données standard qui permettent une communication fluide entre les applications client et serveur. Les protocoles les plus couramment utilisés pour les services web sont HTTP et SOAP (Simple Object Access Protocol)[404]. Ils constituent un moyen normalisé pour les applications logicielles d'interagir entre elles, quels que soient les langages de programmation, les systèmes d'exploitation ou les plates-formes sur lesquels elles sont construites[405]. L'architecture des systèmes d'informations géographiques en ligne est généralement divisée en deux grandes parties. Il y a tout d'abord la couche interne, appelée couche de stockage, qui contient véritablement les données. La protection de la couche interne nécessite un haut niveau de contrôle d'accès, de confiance et une bonne gestion de la confidentialité. Enfin, il y a la couche externe, appelée couche de distribution, où les mesures de sécurité se concentrent sur l'authentification es les utilisateurs et la gestion des privilèges d'accès[406]. Le Web Service doit ainsi assurer la confidentialité, le contrôle d'accès et la gestion de la « vie privée » des données géographiques[407]. C'est le rôle de WS-Security, une norme éditée par l'Organization for the Advancement of Structured Information Standards (OASIS)[408]. La norme WS-Security repose sur trois composantes de sécurité : WS-Trust[409] pour établir une relation de confiance via des jetons de sécurité, WS-Policy[410] qui formalise les spécifications et les attributs des services, et WS-SecureConversation[411]qui garantit des échanges sécurisés et authentifiés. WS-Security ajoute des éléments de sécurité au protocole SOAP pour sécuriser la communication des services web. Ces éléments sont les suivants :

- Identifiant (UsernameToken) : Fournis une authentification basée sur le nom d'utilisateur et le mot de passe.
- Horodatage : Garantis la fraîcheur du message et empêche les attaques par rejeu[412].

---

404 SOAP est un protocole qui utilise XML pour structurer les données et communique via HTTP, SMTP ou TCP. Il est souvent utilisé dans les applications d'entreprise et est connu pour ses normes strictes et ses fonctions de sécurité intégrées. Source : What are Web Services? - A Detailed Guide

405 UnRepo, « What are Web Services? - A Detailed Guide », .https://www.unrepo.com/web-serv/what-are-web-services-a-detailed-guide

406 Xinfeng Ye et Lei Zhong, « Improving web service security and privacy »., In *2011 IEEE World Congress on Services*, pp. 406–413. IEEE, 2011.

407 Zope-Chaudhari Sangita et Venkatachalam P, « Conceptual framework for geospatial data security », International Journal of Database Management Systems, n° 5, p. 29, 2013.

408 OASIS Standard. Ws-secureconversation 1.4, 2009.

409 OASIS Standard. Ws-trust 1.4. http://docs. oasis-open. org/ws-sx/ws-trust/v1, 4, 2009.

410 Curbera Francisco, Hallam-Baker Phillip, VeriSign Maryann Hondo, Nadalin Anthony, Nagaratnam Nataraj, et Sharp Chris, « Web services policy framework (ws-policy) », Policy, 2006.

411 OASIS Standard. Ws-secureconversation 1.4, 2009.

412 Une attaque par rejeu (en anglais, replay attack ou playback attack) est une forme d'attaque réseau dans laquelle une transmission est malicieusement répétée par un attaquant qui a intercepté la transmission. Il s'agit d'un type d'usurpation d'identité. Source : S. van de Beek et F. Leferink, « Vulnerability of Remote Keyless-Entry Systems Against Pulsed Electromagnetic Interference and Possible Improvements », IEEE Transactions on Electromagnetic Compatibility, 1er août 2016, pp. 1259–1265.

- Signature : WS Security signe numériquement certaines parties du message afin d'en garantir l'intégrité.
- Cryptage : Chiffrement des parties du message pour en garantir la confidentialité.

Tout d'abord, pour établir une connexion de confiance, les clients et les fournisseurs d'un service web doivent communiquer avec le STS (service de jetons de sécurité) afin d'émettre, de renouveler et de valider les jetons de sécurité. Ce processus est connu sous le nom de WS-Trust et est régi par les normes OASIS[413]. La deuxième composante est une grammaire polyvalente et extensible utilisée pour décrire les caractéristiques, les spécifications et les attributs généraux des entités dans un système basé sur les services web XML. La troisième norme spécifie les méthodes de création et d'échange de discussion sécurisé ainsi que la manière d'en extraire les clés/jetons afin d'entamer un dialogue sécurisé. Jusqu'à présent, des failles de sécurité spécifiques ont été signalés dans différentes publications[414] et des améliorations futures ont été suggérées pour renforcer la sécurité des données par le biais des services web[415]. L'Open Geospatial Consortium (OGC) participe activement à l'élaboration d'une norme WS dédiée à la diffusion sécurisée des données géographiques en raison de la spécificité de ces dernières. Ainsi, l'OGC Web Service Security (OGC WSS)[416] s'inspire fortement des normes WS-Security, mais avec des schémas XML spéciaux, afin d'assurer une meilleure authentification et d'autres améliorations[417]. D'autres normes participent à la sécurité des services Web et des normes API de l'OGC, comme la norme GeoXACML pour les paramètres d'autorisation que nous verrons plus loin.

En termes généraux, l'anatomie du flux de données entre le client et le serveur web sur internet commence par une requête du navigateur web, du script ou de l'outil du client vers un serveur web hébergeant le site web contenant des documents HTML, des images, des vidéos, des feuilles de style et des fichiers JavaScript, entre autres. L'ensemble de la communication entre le client et le serveur se fait par le biais du protocole de transfert hypertexte (HTTP). Le plus souvent, les serveurs Web transmettent les demandes sous la forme de documents HTML, qui peuvent inclure des images

---

413 L'Organization for the Advancement of Structured Information Standards (OASIS) est un consortium mondial qui travaille pour la standardisation de formats de fichiers ouverts fondés notamment sur XML. Organization for the Advancement of Structured Information Standards — Wikipédia

414 Kaibin Bao, Hristo Valev, Wagner Manuela, et Schmeck Hartmut, « A threat analysis of the vehicle-to-grid charging protocol iso 15118 », Computer Science-Research and Development, 33(1):3–12, 2018.

415 Bertino Elisa, Thuraisingham Bhavani, Gertz Michael, et Damiani Maria Luisa, « Security and privacy for geospatial data »,Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS, Novembre 2008. ; Xinfeng Ye et Lei Zhong, « Improving web service security and privacy ». In 2011 IEEE World Congress on Services, pp. 406–413. IEEE, 2011.

416 Matheus Andreas, « Ogc web services security », 2019.

417 Matheus Andreas, « Testbed-11 engineering report : Implementing common security across the ogc suite of service standards », Technical report, Open Geospatial Consortium, 2015. ; Matheus Andreas, « Testbed-12 ows common security extension er. Technical report », Open Geospatial Consortium, 2016. ; Matheus Andreas et Herrmann J, « Geospatial extensible access control markup langage (geoxacml) », Open Geospatial Consortium Inc. OGC, 2008.

compressées et des scripts en plus du contenu textuel. Les applications Web qui traitent des données non spatiales peuvent ne contenir que des serveurs Web, mais une plateforme de SIG en ligne doit pouvoir fournir des données géoréférencées (c'est-à-dire que chaque point ou élément contient des informations sur sa position sur la Terre) qui seront sous forme de données matricielles (comme le format GeoTiff[418]) ou vecteurs (comme le format shapefile [419]). Cependant, les navigateurs ne sont pas capables d'afficher des données géoréférencées, et sont avant tout développés pour afficher des formats compressés comme PNG, JPG ou GIF qui ne peuvent pas stocker les informations géocodées. Dans le cas d'un SIG en ligne, il est donc nécessaire de disposer d'un autre serveur contenant un moteur SIG capable de convertir des données géoréférencées dans des formats compressés comme PNG, JPG ou GIF qui peuvent être affichés par le navigateur. C'est ce serveur qui forme la couche interne de l'architecture.

Habituellement, un système d'information est installé dans un serveur d'applications qui offre certains services à son utilisateur. L'Open Geospatial Consortium (OGC) a défini un ensemble de normes pour fournir des données géographiques et rendre les couches d'information plus accessibles. Les services web de l'OGC s'articulent autour de fonctions ou commandes, permettant à l'utilisateur de réaliser certaines actions ou de se renseigner sur les données disponibles dans le système d'information avec lequel il interagit. Ainsi, un service de cartographie en ligne se compose de deux fonctions principales : la première est la fonction « Get-Capabilities », qui définit les capacités d'un serveur, telles que les formats de fichiers pris en charge, les couches cartographiques disponibles et la méthode d'affichage. La seconde est la fonction « GetMap », qui indique à la base de données les données cartographiques demandées par le client. La base de données lit une demande et créer les données cartographiques à partir des exigences qui ont été définies par la requête de capacité. Le paquet de données demandé est ensuite envoyé au service de cartographie Web. La norme OGC a permis le développement des services suivants (cf. Figure 14) :

- Service de visualisation (Web Map Service – WMS et Web Map Tile Service – WMTS) : images cartographiques géoréférencées, généralement sous la forme de tuiles raster (PNG, GIF ou JPG). Les tuiles peuvent également être livrées dans un format vectoriel. Les demandes sont effectuées à l'aide d'une adresse URL standard.
- Service de couverture Web (Web Coverage Service – WCS) : une zone géographique qui peut être superposée à une carte, mais qui ne peut pas être modifiée ou analysée. Le WCS est utilisé

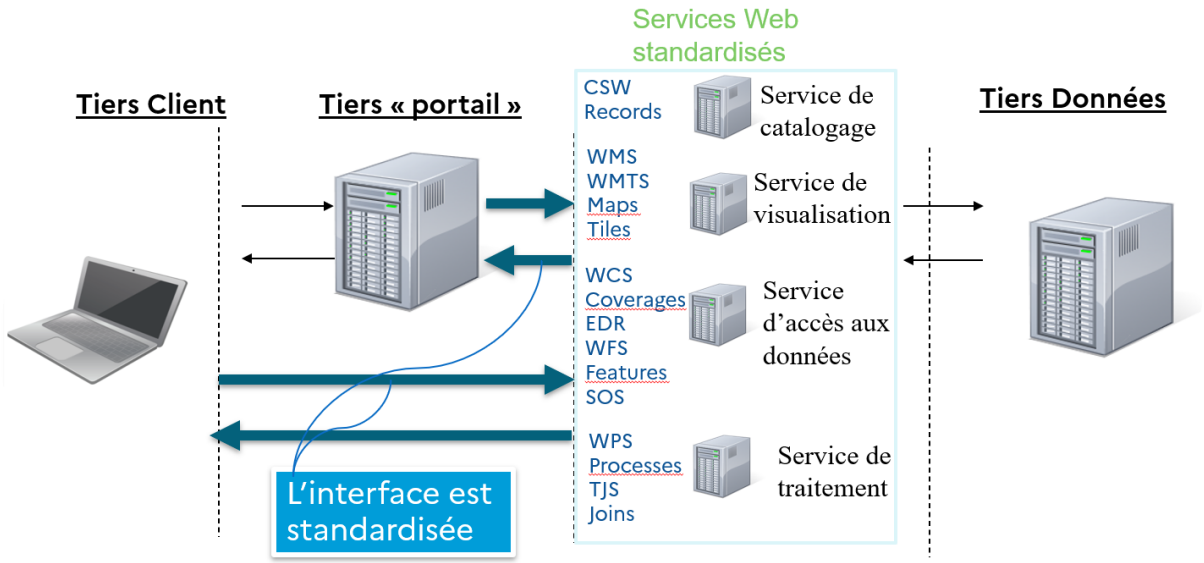
[418] Le GeoTIFF est un standard ouvert permettant d'ajouter des informations de géoréférencement à une image TIFF (projection, système de coordonnées, datation,…). Source : https://archive.wikiwix.com/cache/index2.php

[419] Le Shapefile, développés par Esri, est un format de données vecteurs géospatiales largement utilisé dans les SIG. Ils permettent de représenter des entités géographiques, telles que des points, des lignes et des polygones, et sont compatibles avec de nombreux logiciels SIG. Source : https://help.arcgis.com/en/arcgisdesktop/10.0/help/index.html#/Shapefile_file_extensions/005600000003000000/

pour transférer des couvertures constituées d'objets, tels que des points de données, des pixels ou des chemins définis par des vecteurs.

- Service de catalogage (CSW Records) : permets la découverte, l'exploration et l'exploitation de métadonnées.
- Service d'accès aux données (Web Feature Service – WFS) : permets de demander des caractéristiques géographiques, fournissant essentiellement l'information derrière la carte. Les WFS permettent aux entités d'être interrogées, mises à jour, créées ou supprimées par le client. Ces données sont généralement fournies dans un format XML comme KML ou GML.
- Services de Traitement (WPS Processes) : permets d'exécuter des traitements et processus directement depuis le portail de données sur les données disponibles sur le serveur.

Figure 14 : Les services Web OGC



Source : *IGN, « Les services Web de l'OGC », 2024*

Ainsi, les serveurs SIG en ligne comme GeoServer peuvent fournir les données géographiques à partir d'une variété de formats comme GeoTiff, Shapefile, etc. Les données non spatiales (comme les métadonnées) sont généralement stockées dans une base de données relationnelle et fournissent généralement un langage de requête structuré (comme SQL) pour interroger, manipuler et extraire les données. Les bases de données comme PostgreSQL mettent à disposition de leurs utilisateurs diverses fonctionnalités spatiales avec des extensions comme PostGIS, permettant d'exploiter les caractéristiques spécifiques des données géographiques. Par exemple l'extension géométrique PostGIS permet ainsi, de prendre en charge tous les types de caractéristiques, à savoir les points, les lignes et les polygones. La base de données spatiales est une partie très importante de l'architecture Web-SIG et

permet le stockage et l'interrogation de données liées à des objets dans l'espace, représentés sous forme vecteur ou raster.

La mise en œuvre de SIG en ligne se fait principalement sur un modèle client/serveur. Ce modèle se décline généralement en deux variantes, le « client léger » et le « client lourd ». Dans l'approche « client léger », la plupart des traitements sont effectués par le serveur après une simple demande du client. Et dans l'approche « client lourd », le client dispose de plus de possibilité et peut augmenter ses capacités à l'aide de plug-ins, d'applications tierces ou de modules supplémentaires. Aujourd'hui, la plupart des portails en ligne donnent accès aux informations stockées sur des serveurs distants sur le mode du client « léger », où la majeure partie des traitements s'effectuent sur les serveurs (cf. figure 14). Ces systèmes nécessitent des serveurs SIG, tels que GeoServer, capables de convertir des données géospatiales complexes (vecteurs ou rasters) en formats accessibles par les navigateurs (PNG, JPG, GIF). Ces infrastructures doivent également intégrer des bases de données relationnelles avec extensions spatiales comme PostGIS, permettant de stocker et d'interroger des données géographiques tout en garantissant leur sécurité.

Comme cela vient d'être exposé, l'évolution rapide des technologies numériques et des SIG impose une amélioration constante des pratiques de sécurité. Les acteurs du domaine doivent s'assurer que les principes fondamentaux de sécurité sont respectés. Cela inclut la gestion des accès, la confidentialité des données, et la résilience face aux cyberattaques. Il faut également s'assurer que l'interopérabilité entre les composants soit renforcée, l'adoption cohérente des normes OGC et des extensions comme PostGIS est ainsi cruciale pour garantir la compatibilité entre systèmes. Enfin, les utilisateurs doivent être sensibilisés aux enjeux de la cybersécurité. Les gestionnaires de plateformes SIG doivent également être formés aux normes de sécurité et aux outils disponibles pour minimiser les risques. En intégrant des normes comme celles de l'OGC WSS et WS-Security, et en adoptant des technologies modernes, comme les bases de données relationnelles étendues aux données spatiales, les systèmes d'information géographiques peuvent évoluer pour répondre aux enjeux croissants de sécurité, d'interopérabilité et d'accessibilité. Cela permettra de tirer parti des données géographiques tout en protégeant leur intégrité et leur confidentialité dans un monde de plus en plus interconnecté. Parmi les normes existantes visant à renforcer la résilience des systèmes d'informations géographiques en ligne, les normes OGC WSS et GeoXACML en constituent aujourd'hui le fer de lance.

1.3 Le rôle novateur de l'OGC en matière de cybersécurité : OGC WSS et GeoXACML

Un des rares exemples de standard développé spécifiquement dans le but de renforcer la cybersécurité des systèmes d'information géographiques qui l'implémentent est la norme sur la protection des services Web de l'OGC (OGC Web Service Security), publiée en 2019[420]. L'objectif de la norme de sécurité commune OWS est de permettre la mise en œuvre de mesures de contrôle de la sûreté de l'information et de faire état de leur existence d'une manière interopérable, en ayant un impact minimal sur les mises en œuvre existantes et en adoptant une approche rétrocompatible. La norme s'appuie sur un mécanisme appelé annotation des capacités. Cela signifie que chaque service web décrit ses fonctionnalités de sécurité dans un document que les applications clientes peuvent lire et analyser. Grâce à ce système, un utilisateur peut savoir exactement quelles mesures de sécurité sont mises en place (chiffrement, authentification, etc.)[421], garantissant du même coup l'interopérabilité entre une instance de service Web sécurisé de l'OGC déployée sur HTTPS et une application client. L'approche par l'annotation et le comportement du service en matière de sécurité sont normalisés de manière rétrocompatible afin de garantir qu'ils peuvent être appliqués aux services Web existants de l'OGC sans avoir à modifier les services qui les implémentent déjà.

Ainsi, au sein d'un service web fondé sur les normes OGC (ce qui est le cas de l'immense majorité des infrastructures de données géographiques, à l'exception des cas particuliers utilisant des normes propriétaires), les procédures de sécurité reposent sur la norme OGC Web Service Security. Ce document est une norme d'implémentation pour les services web de l'OGC du protocole de sécurité développée par l'OASIS[422]. Elle évite de rompre l'interopérabilité des services web de l'OGC en standardisant les échanges en fonction des protocoles de sécurité à appliquer. Elle reprend donc toute la nomenclature (à travers la spécification WS-Policy[423]) de chacun des protocoles de sécurité associés aux services web de l'OGC afin que le client et le serveur puissent utiliser le même protocole. Les

---

420 OGC Web Services Security, 17-007r1, 2019. https://www.ogc.org/fr/publications/standard/security/

421 En matière de sécurité, un document de capacités annoté est un document qui utilise le ou les éléments <Constraint> pour exprimer l'existence de contrôles de sécurité sur le fonctionnement de l'instance de service ou la prise en charge d'une caractéristique de sécurité particulière. En résumé, un service peut être décrit par un document de capacités qui comprend des annotations de sécurité telles que définies dans la norme OGC. Un client qui charge ces capacités et analyse les éléments <Constraint> peut déterminer les contrôles de sécurité mis en œuvre pour chaque opération de l'instance de service. (OGC Web Services Security, 17-007r1, 2019).

422 Kelvin Lawrence, Chris Kaler, Anthony Nadalin, R Monzillo, et P Hallam-Baker. « Web services security : Soap message security 1.1 (ws-security 2004) ». OASIS, OASIS Standard, Février 2006.

423 Francisco Curbera, Phillip Hallam-Baker, VeriSign Maryann Hondo, Anthony Nadalin, Nataraj Nagaratnam, et Chris Sharp, « Web services policy framework (ws-policy) ». *Policy*, 2006.

protocoles de sécurité et de communication identifiés par WSS sont les suivants : HTTPS[424]pour le chiffrement des échanges, XACML ou GeoXACML pour le contrôle d'accès basé sur des critères géographiques, OAuth2[425] pour la gestion des autorisations, SAML2[426] et OpenID Connect[427]pour l'authentification. OGC WSS identifie également un certain nombre de menaces potentielles liées à une éventuelle altération des fonctionnalités offertes aux clients du service web et qui peuvent menacer l'intégrité des données offertes par le service où le transfert de données vers et en dehors du service, sur lesquelles nous reviendrons plus en détail dans le chapitre V. Ces vulnérabilités potentielles ont également été mises en avant dans une série de rapports d'ingénierie publiés avant et après la publication de cette norme. Ces documents visent à présenter les objectifs de sécurité visés par les spécifications de la norme [428].

Parmi l'arsenal des profils de normes développées au sein du DGIWG en matière de cybersécurité, le Geospatial eXtensible Access Control Markup Language (GeoXACML) 3.0[429] occupe une place de choix. Cette norme définit une extension géospatiale de la norme OASIS eXtensible Access Control Markup Language (XACML) Version 3.0. Elle permet de définir des politiques d'accès basées sur des critères géographiques en plus des critères classiques, tels que les rôles, les identités ou les attributs utilisateur. GeoXACML vise à fournir un cadre flexible et standardisé pour gérer les permissions d'accès aux données et services géospatiaux. Cette norme prend en compte des scénarios où les politiques d'accès doivent inclure des contraintes géographiques, telles que des zones spécifiques ou des relations spatiales entre des objets. Cela est rendu possible, car GeoXACML étend les fonctions

---

424 L'Hypertext Transfer Protocol Secure (HTTPS, littéralement « protocole de transfert hypertextuel sécurisé ») est la combinaison du HTTP avec une couche de chiffrement TLS 1.3. Source : https://datatracker.ietf.org/doc/html/rfc7568

425 OAuth 2.0 est un protocole d'autorisation et non un protocole d'authentification. En tant que tel, il est principalement conçu comme un moyen d'accorder l'accès à un ensemble de ressources, par exemple, des API distantes ou des données utilisateur. Source : https://auth0.com/fr/intro-to-iam/what-is-oauth-2

426 Security Assertion Markup Language (SAML) est une norme de connexion qui permet aux utilisateurs d'accéder à des applications sur la base de sessions dans un autre contexte. Il s'agit d'une méthode d'authentification unique (SSO) qui offre une authentification plus sûre (avec une meilleure expérience utilisateur) que les noms d'utilisateur et les mots de passe. Source : https://auth0.com/resources/ebooks/saml-authentication-explained?utm_source=google&utm_campaign=emea_france_fra_all_ciam-all_dg-ao_auth0_search_google_text_kw_utm2&utm_medium=cpc&utm_id=aNK4z0000004ITwGAM&utm_term=saml2-c&gad_source=1&gclid=CjwKCAiAneK8BhAVEiwAoy2HYQ2pXyMOtnyclL3khuTFyRq0mIaxsf8eWvLSRTk9MDjqwZpnZGeR8RoCLYUQAvD_BwE

427 OpenID Connect est une simple couche d'identification basée sur le protocole OAuth 2.0, qui autorise les clients à vérifier l'identité d'un utilisateur final en se basant sur l'authentification fournie par un serveur d'autorisation, en suivant le processus d'obtention d'une simple information du profil de l'utilisateur final. Ce processus est basé sur un dispositif interopérable de type REST. En termes techniques, OpenID Connect spécifie une interface HTTP RESTful, en utilisant JSON comme format de données.

428 Andreas Matheus, « Testbed-11 engineering report : Implementing common security across the ogc suite of service standards », Technical report, Open Geospatial Consortium, 2015. ;
Andreas Matheus, « Testbed-12 ows common security extension er. », Technical report, Open Geospatial Consortium, 2016. ;
Andreas Matheus, « Ogc testbed-13: Security er. », Technical report, Open Geospatial Consortium, 2018.

429 Andreas Matheus et J Herrmann, « Geospatial extensible access control markup langage (geoxacml) », Open Geospatial Consortium Inc. OGC, 2008.

du langage XACML pour inclure des critères spatiaux (comme intersecte, contient, au sein de, etc.), permettant de définir des règles comme « Autoriser l'accès uniquement aux données situées dans une zone géographique spécifique ». GeoXACML est développé pour être compatible avec d'autres normes OGC, telles que Web Map Service (WMS), Web Feature Service (WFS) et Web Coverage Service (WCS), assurant ainsi une intégration harmonieuse dans les écosystèmes de plateformes géographiques existants. GeoXACML fait donc partie intégrante des processus de sécurité mis en œuvre dans l'écosystème de l'OGC. Cette norme permet de limiter l'accès à des données géographiques en fonction de leur emplacement. De nombreux cas d'usage existent aujourd'hui concernant l'exploitation des normes OGC WSS et GeoXACML. Ainsi, dans le domaine de la défense et du renseignement, les normes OGC WSS et GeoXACML y sont appliquées pour renforcer la confidentialité et le contrôle d'accès selon les classifications de sécurité. À titre d'exemple, l'OTAN, via les travaux menés par le Defence Geospatial Information Working Group (DGIWG), a profité d'OGC WSS pour gérer le concept de données classifiées sur des services OGC. Un profil DGIWG pour WFS indique dans le document de capacités (Capabilities) le plus haut niveau de classification des données disponibles via l'élément <AccessConstraints>[430]. Concrètement, un service WFS militaire peut annoncer qu'il contient des données jusqu'au niveau Confidentiel par exemple, et n'exposera la liste des couches qu'à un client authentifié ayant les droits adéquats. En effet, dans un cas d'usage de type « service protégé / données privées / catalogue public », la norme WSS prévoit que le GetCapabilities public ne liste pas le contenu sensible tant que le client n'a pas prouvé son identité et son autorisation[431]. Ce mécanisme implémente le principe de « besoin d'en connaître ». Un utilisateur non autorisé ne voit même pas qu'une couche confidentielle existe. Une fois authentifié via les mécanismes WSS (certificat, SAML, etc.), le client peut accéder aux couches en respectant les contraintes de sécurité annoncées. En complément, GeoXACML apporte le contrôle d'accès géographique fin dans ces scénarios militaires. Ainsi, il peut être défini que « l'utilisateur X ne peut interroger la couche d'intelligence que sur sa zone d'opération définie ». Techniquement, une politique GeoXACML contiendra une condition spatiale limitant la requête WFS aux géométries à l'intérieur du périmètre autorisé pour cet utilisateur. Ce type de règle a été exploré lors d'exercices OGC. Un rapport de testbed mentionne l'utilisation d'un moteur GeoXACML comme PDP pour filtrer les entités renvoyées par un service selon la zone autorisée[432]. De plus, dans les systèmes de cartographie militaire multiniveaux, GeoXACML permet d'harmoniser les politiques d'accès entre différentes nations ou services en utilisant un langage standard commun plutôt

---

430 Open Geospatial Consortium, « OGC Web Service Security », OGC 17-007r1, version 1.0, 28 janvier 2019, p.18.

431 Ibid.

432 Herrmann Jan, « Access Control for OGC Web Services with (Geo)XACML », 69th OGC Technical Committee Meeting Massachusetts Institute of Technology Cambridge, USA, 23 juin 2009. https://www.slideserve.com/sari/access-control-for-ogc-web-services-with-geo-xacml. Consulté le 12 mars 2024.

que des solutions ad hoc propres à chaque système[433].En somme, dans le domaine militaire, OGC WSS et GeoXACML assurent que seules les personnes habilitées, disposant du bon niveau de clearance et situées dans le bon contexte opérationnel, accèdent aux données géospatiales sensibles, tout en maintenant l'interopérabilité entre systèmes alliés. OGC WSS Security et GeoXACML jouent donc un rôle crucial pour garantir un contrôle d'accès précis et sécuriser dans les environnements SIG, tout en assurant une interopérabilité maximale entre les systèmes et services.

Ainsi, la norme OGC WSS apporte une réponse essentielle aux défis de sécurité des systèmes géographiques. Elle garantit une interopérabilité universelle, protège les données sensibles, et offre des outils performants pour sécuriser les échanges. Grâce à son intégration des standards internationaux de cybersécurité, comme OAuth et GeoXACML, elle s'est imposée comme une référence pour protéger les services web géographiques dans un monde interconnecté. Ces efforts contribuent non seulement à sécuriser les infrastructures critiques, mais aussi à établir un langage commun pour gérer les accès et les données dans un écosystème global. Cette nécessaire amélioration des pratiques de sécurité et d'interopérabilité dans les systèmes d'information géographiques s'inscrit dans un contexte où la question de la valeur légale des données géographiques gagne en importance. Alors que ces données sont de plus en plus diffusées, tant par des organismes étatiques que par des acteurs privés, il devient essentiel de clarifier leur portée juridique et de déterminer lesquelles peuvent être considérées comme officielles, notamment au regard des enjeux de souveraineté qui sous-tendent à leur création et à leur diffusion.

[433] Matheus Andreas, « Geospatial eXtensible Access Control Markup Language (GeoXACML) », W3C PLING Meeting, Universität der Bundeswehr München, 2009. https://www.w3.org/Policy/pling/wiki/images/5/59/GeoXACML.pdf. Consulté le 12 mars 2024.

2. La protection des données géographiques : des enjeux en matière de responsabilité juridique et de souveraineté

La portée juridique de la production de données géographiques n'est pas nécessairement évidente. Contrairement à la façon dont le commun conçoit généralement la valeur légale des informations géographiques diffusées par les instances étatiques et les autorités « reconnus » comme l'IGN, leur portée juridique n'est pas implicite. Toutes les informations géographiques produites par les administrations nationales n'ont pas de portées juridiques légales. Avec la diffusion accélérée des informations géographiques à la fois par des organes nationaux et des sociétés privées telles que Google, déterminer quelles sont les informations géographiques reconnues comme « légales » au sens juridique du terme devient essentiel et permet de déterminer autour de quelles données gravitent les enjeux de souveraineté importants.

Certaines données géographiques ont une portée juridique reconnue par diverses lois, décrets ou arrêtés comme dans le cas des données géodésiques de base qui bénéficient d'une protection législative et réglementaire, comme souligné par Verdier[434] : « s'ajoutent ainsi par exemple au Décret relatif à la géodésie [435] l'Arrêté du 16 septembre 2003 portant sur les classes de précision applicables aux catégories de travaux topographiques réalisés par l'État, les collectivités locales et leurs établissements publics ou exécutés pour leur compte[436], et, bien entendu, la reconnaissance législative, et ancienne, de mission de service public confiée aux géomètres-experts et des données produites dans ce cadre [437]. Bien sûr, il faut citer certains « documents graphiques » notamment ceux contenus dans les plans locaux d'urbanisme qui se sont vus, progressivement, reconnaître une valeur et une opposabilité juridique en tant que telles. Sans omettre de mentionner la reconnaissance législative de « l'infrastructure d'information géographique » circonscrite au Droit de l'Environnement et intégrée au chapitre VII du Titre II « Information et participation des citoyens » du Livre Ier du Code de l'Environnement, qui a, notamment, pour mérite de poser une définition législative de la donnée géographique »[438]. Cependant, bien que certaines données géographiques bénéficient d'un cadre

---

434 Amelle Verdier, « La portée juridique de l'information géospatiale dans la jurisprudence administrative et civile », Afigéo, mars 2019.

435 Décret n° 2019-165 du 5 mars 2019 relatif au système national de référence de coordonnées (JORF n° 0056 du 7 mars 2019 texte n° 4) et Décret n° 2006-272 du 3 mars 2006 modifiant le Décret n° 2000-1276 du 26 décembre 2000, *portant application de l'article 89 de la Loi n° 95-115 du 4 février 1995 modifiée d'orientation pour l'aménagement et le développement du territoire relatif aux conditions d'exécution et de publication des levés de plans entrepris par les services publics*, JORF n° 59 du 10 mars 2006, page 3623.

436 Arrêté du 16 septembre 2003, *portant sur les classes de précision applicables aux catégories de travaux topographiques réalisés par l'État, les collectivités locales et leurs établissements publics ou exécutés pour leur compte*, JORF n° 252 du 30 octobre 2003, page 18546.

437 Loi n° 46-942 du 7 mai 1946 instituant l'Ordre des géomètres experts.

438 Amelle Verdier, Op. cit.

juridique explicite et reconnu, d'autres ne sont pas directement encadrées par des textes spécifiques, mais leur utilisation dans des contextes judiciaires n'en est pas pour autant exclus, et illustre leur importance croissante. En effet, qu'il s'agisse de recours en droit de l'urbanisme ou d'autres litiges, ces données peuvent jouer un rôle clé dans l'établissement des faits, soulignant ainsi l'importance de garantir leur fiabilité, leur accessibilité et leur protection contre d'éventuelles manipulations frauduleuses.

2.1 Les différentes modalités encadrant la valeur juridique des données géographiques

Il est vrai que toutes les données produites ne sont pas encadrées par des textes juridiques explicites. Malgré cela, certaines données géographiques ont déjà été utilisées pour appuyer certains recours en justice, notamment dans le Droit de l'urbanisme. Ainsi, des relevés cartographiques ou des photographies peuvent être utilisés afin de justifier d'un recours en justice concernant l'usage, l'occupation ou la jouissance d'un bien immobilier. Ainsi, la décision du Conseil d'État du 13 avril 2016, concernant l'annulation d'un permis de construire, s'est appuyé sur des plans de l'espace concerné afin de déterminer les dommages éventuels que pouvait causer la poursuite des travaux pour la partie ayant initialement saisi le tribunal administratif de Marseille[439]. D'autres documents relevant des données géographiques produites par l'IGN et les collectivités locales peuvent également être présentés comme preuve lors de procès, comme les relevés du cadastre ou même des images issues du Géoportail de l'urbanisme ou de la Géoplateforme nationale. À titre d'exemple, la circulaire ministérielle n° 2015-101 du 9 juin 2015[440] précise que les modalités d'attribution des bourses en fonction de l'éloignement du domicile familial doivent se faire en consultant uniquement le répertoire des communes de l'IGN et/ou le fichier de la Poste. L'ensemble de ces documents étant mis à la disposition du public via les services de SIG en ligne, en conserver le bon fonctionnement et la disponibilité est capital pour permettre l'usage de ces données par les citoyens qui peuvent s'avérer essentiels pour résoudre des conflits. Il peut également arriver que des tentatives de fraude soient dénoncées, notamment lors des études d'impact pour l'installation de parc éolien qui reposent sur l'emploi de cartes de visibilités et de photographies qui peuvent être truquées.

Si des déplacements sur le terrain peuvent permettre de trancher certains litiges que les cartes et images ne permettraient pas de résoudre, ces derniers sont rares et pas toujours faisables lors du procès. De fait, les représentations cartographiques et les photomontages constituent donc souvent des

---

[439] Verdier Armelle, *Op. cit.*

[440] Conseil d'État, 1ère - 6ème chambres réunies, 13/04/2016, 389798, *Publié au recueil Lebon*. https://www.legifrance.gouv.fr/ceta/id/CETATEXT000032405469/. Consulté le 3 mai 2024.

éléments employés pour justifier d'une décision de justice, alors que ni les images du cadastre ni celles issues de la Géoplateforme de l'IGN n'ont officiellement de portée juridique. C'est donc la décision des juges d'employer des données issues de ces géoplateformes qui hissent ces données au rang de preuves les données géographiques.

Ainsi, aujourd'hui, les données géographiques peuvent constituer des éléments de preuve, mais ce n'est pas le cas de l'ensemble des données géographiques disponibles. De fait, les éléments fournis par une carte touristique ne peuvent être utilisés comme éléments de preuve concernant les litiges attenants à des limites communales ou régionales, car ces dernières ne peuvent avoir de portée que « purement informative »[441]. Cependant, si les données géographiques publiées par le site internet de l'IGN ainsi que sur le Géoportail ou la Géoplateforme sont également publiées à titre d'information, à l'exclusion de toute garantie sur leur exactitude, celles-ci ont déjà été utilisées comme élément de preuve (toujours à l'appui d'autres éléments concordants), car jugées suffisamment fiables, complètes et récentes pour être admises comme élément de preuve. Un exemple concret illustrant la valeur probatoire des données géographiques IGN a été donné par une ordonnance de référé de la Cour d'appel de Montpellier du 29 novembre 2018 (n° 17/06604). Dans cette affaire, des particuliers (époux X) contestaient la présence d'un hangar à chevaux trop proche de leur habitation, en violation d'une distance minimale de 50 mètres imposée par le règlement sanitaire départemental. Pour prouver que le hangar se situait bien à moins de 50 m, ils ont produit aux débats des relevés de distance extraits du site Géoportail (géré par l'IGN). La partie adverse s'est opposée à cet usage, soutenant « qu'il ne peut être tenu compte d'un document Géoportail produit par la partie adverse (…), ce type de document posant question sur la précision récente des données collectées par ce site et sur l'exactitude des données qui n'est pas garantie »[442]. En d'autres termes, les défendeurs invoquaient le caractère purement informatif des données du Géoportail pour en contester la fiabilité. Malgré cette contestation, la Cour a estimé que les données issues du Géoportail de l'IGN étaient suffisamment fiables pour être admises comme preuve, aux côtés d'autres éléments (constats d'huissier, cadastre, photographies). Le juge relève en effet que si le site Géoportail mentionne l'absence de garantie quant à l'exactitude des informations, il précise aussi la grande qualité et la mise à jour constante de ses données officielles. L'indication fournie par les services de l'IGN concernant la nature purement informative des informations postées sur leurs sites internet n'exclut donc pas leur usage comme élément de preuve et ne supprime pas

[441] Circulaire n° 2015-101 du 9-6-2015, « Modalités d'attribution des bourses d'enseignement supérieur sur critères sociaux et des aides à la mobilité internationale pour l'année 2015-2016 », NOR : MENS1509669C, MENESR - DGESIP A2-1.
[442] Arrêt de la Cour Administrative d'Appel de Lyon, Req. n° 11LY01784, 5 avril 2012.

entièrement toute forme de responsabilité concernant les exigences d'exactitude de ces données au vu de la jurisprudence actuelle.[443] [444]

Il existe également des données géographiques dont la portée juridique est incontestable, en particulier lorsque ces données concernent des plans de prévention des risques (PPR), dont les inexactitudes et manquements pourraient entraîner des conséquences graves pour des personnes et/ou des biens. De fait, des erreurs dans l'établissement d'un plan de prévention des risques par les services de l'État peuvent engager sa responsabilité en cas de dommages liés à un risque naturel [445]. Dans un autre domaine, la cartographie des réseaux souterrains d'eau et d'électricité s'appuie à l'échelle nationale, sur le Plan Corps de rue simplifié à très grande échelle (PCRS), qui a été normalisé grâce aux travaux du Conseil national de l'information géolocalisée (CNIG) depuis juin 2015, et dont la deuxième version a été publiée en septembre 2017. Depuis la publication de l'arrêté du 22 décembre 2015, relatif au contrôle des compétences des personnes intervenant dans les travaux à proximité des réseaux et modifiant divers arrêtés relatifs à l'exécution de travaux à proximité des réseaux, *« Le fond de plan employé pour la transmission des données de localisation des réseaux aux déclarants est le meilleur lever régulier à grande échelle disponible, établi et mis à jour par l'autorité publique locale compétente en conformité avec les articles L. 127-1 et suivants du code de l'environnement et selon le format d'échange PCRS (plan corps de rue simplifié) établi et mis à jour par le Conseil national de l'information géographique »*[446]. La simplification et la diffusion d'un même plan corps de rue simplifié grâce aux travaux de normalisation du CNIG a permis l'amélioration de la cartographie de l'ensemble des réseaux souterrains du territoire. Elle a aussi permis de constituer une base nationale de référence reconnue par la justice en cas d'incident lors de travaux à proximité des réseaux enterrés et aériens. La responsabilité en cas de dommage infligé aux réseaux souterrains ou aux biens de tiers reposant sur les maîtres d'ouvrage, la généralisation de l'emploi du PCRS permet de réduire fortement les risques de dommages tout en constituant un référentiel reconnu par la justice en cas de litige lors des travaux.

Ainsi, il existe plusieurs types de données géographiques considérées comme légales selon différentes modalités. Comme le soulignait déjà Verdier en 2019[447], les données géographiques peuvent être légales « par détermination » et/ou « par effets juridiques »[448]. On peut dire qu'une donnée est

[443] Cour d'appel de Montpellier, 1ère chambre d, 29 novembre 2018, n° 17/06604. https://www.doctrine.fr/d/CA/Montpellier/2018/CB7BD2A027B2B1BF33F5F.

[444] Verdier Armelle, « La portée juridique de l'information géospatiale dans la jurisprudence administrative et civile », *Afigéo*, mars 2019.

[445] CAA Marseille, 7 févr. 2008, n° 05MA01729 – CAA Douai, 15 nov. 2007, n° 06DA00335.

[446] Arrêté du 22 décembre 2015 relatif au contrôle des compétences des personnes intervenant dans les travaux à proximité des réseaux et modifiant divers arrêtés relatifs à l'exécution de travaux à proximité des réseaux.

[447] Verdier Armelle, « L'information géospatiale légale : (1/2) 1. Synthèse des contributions », *Afigéo*, p. 1, juillet 2019.

[448] Ibid.

légale par détermination lorsqu'elles sont reconnues par la loi comme étant réglementaires ou seules capables de faire foi. On peut regrouper dans cette catégorie les cartes de vol pour les aéronefs, ou encore les cartes maritimes normalisées par l'IHO. On peut également y ajouter les données des Plans locaux d'urbanisme (PLU) et les schémas de cohérence territoriale (SCoT). Ainsi, il peut exister un consensus sur la valeur juridique de certaines données, considérées comme suffisamment fiables pour faire office de preuve, sans nécessairement que cela soit explicitement présenté comme tel dans la loi. Certaines données géographiques acquèrent une valeur juridique par « effets juridiques induits »[449]. Ces dernières sont des données opposables à un tiers, comme les frontières internationales et infranationales (régions, parc national, limites d'installations militaires). Lorsque ces données sont employées afin de faire valoir les droits des personnes, elles acquièrent un caractère juridiquement opposable. Enfin il existe des données dont la qualification juridique est garantie par la réglementation.

La production de données géographiques de qualité, normalisée et maintenue disponible pour les citoyens, constitue donc un enjeu stratégique dans certains domaines, notamment du point de vue juridique. Aujourd'hui, à quelques exceptions près (lorsque les données sont soutenues par des textes de loi précis), la valeur juridique des informations géographiques est fixée par la jurisprudence, qui grave dans le droit l'usage juridique de certaines données. La valeur juridique des données géographiques est donc décidée en aval et non en amont de son processus de production, ce qui soulève des enjeux de souveraineté. De fait, la maîtrise du cycle de production de ces données, qui peuvent être amenées, de plus en plus, à déterminer des décisions de justice, doit faire l'objet d'une attention continuelle, en ce qu'elles participent à modeler la façon dont se construit le droit. La normalisation est ici un outil puissant pour garantir la diffusion de modèles de données de référence et contrôlés, permettant de garantir l'exactitude des données diffusées par les services de l'État et les sociétés privées affiliées à leur production. Le poids juridique de certaines informations géographiques invite également à se soucier sérieusement de leur protection et de leur diffusion auprès des citoyens qui doivent être en mesure de disposer de l'ensemble des données leur permettant d'ester en justice, en toute circonstance.

Ainsi, toutes les données géographiques n'ont pas la même portée juridique. Certaines, comme les cartes touristiques ou les visualisations issues de services privés, sont considérées comme purement informatives et ne sauraient, à ce titre, fonder une décision de justice ou une action administrative. D'autres, bien qu'également publiées avec une clause de non-responsabilité, comme celles de l'IGN via le Géoportail ou la Géoplateforme, peuvent néanmoins être admises à titre de preuve lorsqu'elles présentent des caractéristiques suffisantes de fiabilité, d'actualisation et de précision, comme l'illustre

[449] Ibid.

la jurisprudence récente. Ces décisions démontrent que l'absence de portée normative explicite n'exclut pas une recevabilité conditionnée par la qualité technique et l'usage en contexte probatoire. Toutefois, cette dimension juridique ne peut être dissociée des conditions de sécurité dans lesquelles ces données sont produites et conservées. Dans un environnement numérique soumis à des risques croissants de falsification, de compromission ou d'usurpation d'identité numérique, la capacité à garantir l'intégrité et la traçabilité des données devient un critère central de leur admissibilité juridique. Une donnée géographique altérée à la suite d'un incident de cybersécurité pourrait perdre toute valeur probante, tandis qu'un défaut de contrôle sur les accès ou les modifications pourrait faire peser une responsabilité sur l'entité productrice ou gestionnaire. En ce sens, le développement et l'adoption de normes techniques de cybersécurité (telles que les standards OGC WSS ou GeoXACML) ne relèvent pas uniquement de la sphère technique, ils participent d'une architecture juridique implicite, où la fiabilité technique fonde la recevabilité légale. La normalisation des dispositifs de sécurisation des données géographiques numériques constitue ainsi un levier essentiel pour articuler exigences de souveraineté, de protection contre les risques cyber et reconnaissance juridique des données dans les usages administratifs, contentieux ou réglementaires.

À ce sujet, la protection des données géographiques numériques apparaît comme un problème de premier plan pour l'État, qui est historiquement le premier fournisseur et producteur de données géographiques. La sauvegarde des données géographiques numériques contre de potentielles attaques cyber relève aujourd'hui du rôle de l'État, notamment concernant celles mises à la disposition du public et les données nécessaires à l'aménagement du territoire. Avec l'émergence d'un grand nombre d'acteurs privés dans le milieu de la collecte et de la transformation des données géographiques, la question de l'érosion éventuelle de la notion de gouvernance concernant ces données finit par se poser.

2.2 Gouvernance et protection des données

La production et la diffusion des données géographiques n'ont jamais constitué une activité neutre du point de vue de la gouvernance. Dans le modèle traditionnel qui a longtemps prévalu, la chaîne de valeur géospatiale s'inscrivait dans le cadre d'une organisation clairement hiérarchisée, au sein de laquelle les pouvoirs publics exerçaient un contrôle quasi exclusif sur chacune de ses étapes. La production de données géographiques repose en effet historiquement sur un écosystème d'acteurs institutionnels opérant à différents échelons du territoire, depuis les communes jusqu'aux agences nationales[450]. Ainsi, les collectivités territoriales, qu'elles soient régionales ou municipales, assurent la production et la mise à jour de référentiels locaux portant aussi bien sur les caractéristiques du bâti et des infrastructures que sur le tracé des limites administratives ou encore sur des attributs socio-économiques géolocalisés tels que les données de santé ou les indicateurs d'activité économique[451]. Dans ce cadre, les autorités publiques collectent, valident et mettent à disposition des données géospatiales à la fois pour leurs propres usages administratifs et pour des tiers autorisés opérant dans le cadre de licences encadrées[452]. Ce système confère aux pouvoirs publics une maîtrise d'ensemble sur l'intégralité du cycle de production, depuis l'acquisition jusqu'à la diffusion des données géographiques.

Ce régime d'organisation de la donnée géographique n'a toutefois pas résisté aux bouleversements induits par la transition numérique. La montée en puissance d'acteurs privés dans ce domaine, conjuguée à la généralisation des plateformes en nuage et à l'essor des données massives, a profondément reconfiguré les rapports de force entre institutions publiques et opérateurs privés en matière de production et de contrôle des données géographiques. C'est dans ce contexte que la notion de souveraineté des données géographiques a acquis, au cours de la dernière décennie, une acuité particulière, tant dans les travaux académiques que dans les arènes politiques européennes. L'émergence du Règlement général sur la protection des données (RGPD)[453], du système européen de certification de cybersécurité pour les services en nuage (EUCS)[454], du projet Gaia-X[455] ou encore des

---

[450] Budhathoki Nama Raj, Bruce Bertram (Chip), et Nedovic-Budic Zorica, « Reconceptualizing the role of the user of spatial data infrastructure », GeoJournal, n°72, 2008, p. 149-160.

[451] Harvey F., et Tulloch D., « Local-government data sharing: Evaluating the foundations of spatial data infrastructures », International Journal of Geographical Information Science, 20, 2006, p. 743-768.

[452] Kulk Stefan, et Van Loenen Bastiaan, « Brave new open data world? », International Journal of Spatial Data Infrastructures Research, 7, 2012, p. 196-206.

[453] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). https://eur-lex.europa.eu/legal-content/FR/TXT/

[454] Commission européenne, « Implementing Regulation on the adoption of a European Common Criteria-based cybersecurity certification scheme », 31 janvier 2024. https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-adoption-european-common-criteria-based-cybersecurity-certification-scheme

[455] https://gaia-x.eu/

espaces communs européens de données[456] témoigne de la volonté des institutions européennes de réaffirmer un cadre normatif face à des dynamiques qui leur échappent partiellement. Le Patriot Act américain de 2001 en offre une illustration saisissante : en autorisant les agences fédérales américaines à accéder à toute donnée hébergée par des prestataires relevant du droit américain, y compris lorsque ces données sont physiquement situées hors du territoire des États-Unis, et en interdisant à ces prestataires de divulguer l'existence de tels accès, cette législation consacre une forme d'extraterritorialité de la souveraineté numérique américaine directement antagoniste aux ambitions européennes[457].

La multiplication des flux transfrontaliers de données a ainsi transformé la souveraineté de la donnée en un problème juridique de première importance pour les États. Car la revendication de souveraineté sur des données géographiques ne se limite pas à une question de principe, elle peut également être appelée à produire des effets concrets dans des contextes contentieux. La contre-cartographie, qui consiste à opposer des ensembles de données géospatiales historiques à des prétentions territoriales adverses, a notamment été mobilisée aussi bien dans des règlements informels que dans des litiges formels[458]. Or, pour qu'une telle démarche soit juridiquement opérante, encore faut-il être en mesure de démontrer l'authenticité et l'intégrité des données invoquées, ce qui suppose une traçabilité et une protection robustes de ces données tout au long de leur cycle de vie. L'affaire du Health Data Hub illustre de manière particulièrement parlante les tensions que cette situation engendre dans le contexte français[459]. Cette configuration place les institutions françaises dans une situation paradoxale, en ce qu'elles sont productrices de données souveraines par vocation tout en étant susceptibles d'en perdre le contrôle effectif du seul fait des architectures techniques et contractuelles dans lesquelles ces données sont inscrites

C'est dans ce contexte d'affaiblissement progressif du contrôle étatique sur la donnée géographique que s'inscrit la montée en puissance d'opérateurs privés dans la production de référentiels spatiaux. Les grandes plateformes numériques que sont Google, Apple ou Microsoft se sont en effet

---

[456] Commission européenne, « Common European Data Spaces », 10 octobre 2024. https://digital-strategy.ec.europa.eu/en/policies/data-spaces

[457] Barrett Lindsey, « Confiding in con men: US privacy law, the GDPR, and information fiduciaries », Seattle University Law Review, 42, 2018. https://digitalcommons.law.seattleu.edu/sulr/vol42/iss3/5/

[458] Amelle Verdier, « La portée juridique de l'information géospatiale dans la jurisprudence administrative et civile », Afigéo, mars 2019.

[459] Le Health Data Hub (HDH) est un groupement d'intérêt public créé par la loi n°2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé. Dès novembre 2019, le gouvernement a confié l'hébergement à Microsoft Azure, sans appel d'offres européen. La CNIL a exprimé ses préoccupations en juin 2020 en raison de l'incompatibilité du Cloud Act américain de 2018 avec le droit européen. Voir : Conseil d'État, ord. réf., 19 juin 2020, n°440916 ; Conseil d'État, ord. réf., 21 septembre 2020, n°444514 ; CJUE, 16 juillet 2020, Data Protection Commissioner c. Facebook Ireland Ltd et Maximillian Schrems, aff. C-311/18.

progressivement constituées en acteurs centraux de la production de données géographiques, souvent en s'appuyant sur des fonds publics mis à disposition sous des licences ouvertes permettant leur réutilisation dérivée, telle la Licence Ouverte 2.0 en vigueur en France[460] [461]. Microsoft a par exemple rendu accessibles, sous forme de jeux de données ouverts, des ensembles d'empreintes de bâtiments générés automatiquement par analyse d'imagerie satellitaire à l'échelle de pays entiers[462]. De la même manière, la constitution de réseaux d'imagerie au niveau de la rue, initiée par Google Maps/Street View et reprise notamment par Apple Maps ou par le projet de cartographie participative Mapillary, témoigne de la capacité des acteurs privés à mobiliser des ressources de collecte que les États ne peuvent égaler[463]. Cette compétition asymétrique nourrit une dépendance croissante des administrations publiques envers des données dont elles ne maîtrisent ni les conditions de production ni les modalités de mise à disposition[464]. Les gouvernements conservent certes un rôle de régulateur[465], mais la capacité à exercer effectivement ce rôle suppose une maîtrise technique et juridique que la fragmentation croissante du paysage de la donnée géographique rend de plus en plus difficile à maintenir.

Il est également à noter que ces évolutions donnent toute leur acuité à la notion de souveraineté de la donnée, dont les travaux de recherche récents ont souligné le caractère polysémique et les implications multidimensionnelles[466]. D'une part, les accords commerciaux internationaux comportent des clauses de libre circulation des données qui limitent la capacité des gouvernements à restreindre les flux transfrontaliers[467]. D'autre part, de nombreux pays cherchent à renforcer leur emprise sur les données par des dispositifs de localisation[468]. L'exemple de l'ambassade de données estonienne au Luxembourg illustre les solutions originales que certains États explorent pour concilier exigences de continuité numérique et impératifs de souveraineté[469]. Cette question touche à des dimensions fondamentales de la souveraineté nationale : la capacité des États à garantir à leurs ressortissants la

---

[460] Rhind David W., « National and international geospatial data policies », In Geographical information systems: Principles, techniques, management and applications, Volume 2: Management issues and applications, 1999, p. 767-787.

[461] https://www.etalab.gouv.fr/wp-content/uploads/2017/04/ETALAB-Licence-Ouverte-v2.0.pdf

[462] https://github.com/microsoft/IdMyPhBuildingFootprints

[463] Alvarez Leon Luis F., et Quinn Sterling, « The value of crowdsourced street-level imagery: Examining the shifting property regimes of OpenStreetCam and Mapillary », GeoJournal, n°84, 2019, pp. 395-414.

[464] Taylor Linnet, « Public actors without public values: Legitimacy, domination and the regulation of the technology sector », Philosophy & Technology, n°34, 2021, pp. 897-922.

[465]Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[466] Hummel Patrick, Braun Matthias, Tretter Max, et Dabrock Peter, « Data sovereignty: A review », Big Data & Society, 8, 2021. https://journals.sagepub.com/doi/10.1177/2053951720982012

[467] McCann David, « E-commerce free trade agreements, digital chapters and the impact on labour », International Trade Union Confederation, 2019.

[468] Chander Anupam, et Lê Uyen P., « Data nationalism », Emory Law Journal, n°64, 2019, pp. 677-740.

[469] Rice Nikolai F., « Estonia's digital embassies and the concept of sovereignty », Georgetown Security Studies Review, 2019.

protection de leurs données personnelles[470], la volonté de certains gouvernements de conserver le contrôle de leurs réserves de données nationales pour soutenir une économie de l'innovation endogène[471], ou encore l'aspiration à faire des données publiques un levier de développement économique national[472]. La notion de localisation des données, souvent comprise comme l'exigence que les données soient physiquement hébergées dans la juridiction de l'État concerné, permet d'empêcher l'accès par des appareils de sécurité d'États tiers[473] et garantit l'accès opérationnel rapide des autorités nationales[474]. Or la migration massive des données publiques vers des services en nuage remet en cause ces garanties[475], en transformant la donnée d'une propriété tangible à une ressource soumise à des conditions contractuelles impliquant un transfert variable du contrôle vers des tiers hébergeurs[476].

Face à ces reconfigurations, la littérature académique a cherché à doter les analystes d'outils conceptuels permettant de décrire et de comparer les régimes de gouvernance de la donnée géographique. Ces tentatives de typologisation sont multiples et obéissent à des logiques différentes. Certains travaux ont proposé de distinguer les régimes selon la nature des acteurs revendiquant la souveraineté, en différenciant les approches étatiques, les revendications d'acteurs privés et les mouvements issus de la société civile[477]. D'autres ont construit leurs typologies à partir des valeurs sous-jacentes aux différentes conceptions de la souveraineté numérique, distinguant par exemple un modèle fondé sur les droits individuels, un modèle orienté marché, un modèle de centralisation étatique et un modèle de souveraineté d'État stricto sensu[478]. Ces approches sont intéressantes, mais elles demeurent très générales et s'appliquent à l'ensemble du domaine numérique sans s'attacher aux spécificités du secteur des données géographiques. C'est précisément le mérite des travaux de Johnson et Scassa (2023) que de proposer une grille d'analyse spécifiquement centrée sur la donnée spatiale[479].

---

[470] Baezner Marie, et Robin Patrice, « Cyber sovereignty and data sovereignty », ETH Zurich, 2018.

[471] Singh Vikram Jeet, et Bhatia Kalindhi, « India: What's driving data localisation in India? », BTG Legal, 2020.

[472] Aggarwal Sachin, « Treasure of the commons: Global leadership through health data », Centre for International Governance Innovation, 2018.

[473] Fantin S., « Data Protection Commissioner v Facebook Ireland Limited », European Data Protection Law Review, n°6, 2020, pp. 325-331.

[474] Daskal J., « Law enforcement access to data across borders: The evolving security and rights issues », Journal of National Security Law and Policy, n°8, 2016, pp. 473-502.

[475] Ashton Philippe, Weber Rachel, et Zook Matthew, « The cloud, the crowd, and the city: How new data practices reconfigure urban governance? », Big Data & Society, n°4, 2017.

[476] Leszczynski Agnieszka, « Speculative futures: Cities, data, and governance beyond smart urbanism », Environment and Planning A: Economy and Space, n°48, 2016, pp. 1691-1708.

[477] Johnson Peter A. et Scassa Teresa, « Who owns the map? Data sovereignty and government spatial data collection, use, and dissemination », Transactions in GIS, n°27, 2023, pp. 275-296. https://onlinelibrary.wiley.com/doi/abs/10.1111/tgis.13024

[478] Thorsby Jeffrey, Stowers Genie N. L., Wolslegel Kristen, et Tumbuan Ellie, « Understanding the content and features of open data portals in American cities », Government Information Quarterly, n°34, 2017, pp. 53-61.

[479] Janssen Marijn, Charalabidis Yannis, et Zuiderwijk Anneke, « Benefits, adoption barriers and myths of open data and open government », Information Systems Management, n°29, 2012, pp. 258-268.

En organisant les régimes de gouvernance géospatiale sur un continuum allant du contrôle étatique intégral au désengagement complet de l'État, ces auteurs identifient quatre modèles, dont la logique sera reprise ici tout en les éclairant par des exemples complémentaires tirés du contexte français et européen.

Selon Johnson et Scassa, le premier modèle est celui dans lequel le gouvernement assume l'intégralité de la responsabilité du système géospatial national, depuis la collecte jusqu'à la diffusion des données[480]. Dans ce cadre, l'État assure non seulement la production des données, mais aussi leur mise à disposition contrôlée, selon un régime de recouvrement des coûts ou d'accès libre, conformément aux priorités et aux politiques du gouvernement[481]. Les portails de données ouvertes mis en place par les administrations nationales en sont la déclinaison contemporaine[482]. Ce modèle maximise le contrôle étatique sur la chaîne de valeur géospatiale. Nombre de gouvernements ont toutefois été critiqués pour avoir maintenu un contrôle trop exclusif sur leurs données, freinant ainsi leur réutilisation[483]. C'est précisément la raison qui a poussé l'État français à ouvrir gratuitement l'ensemble des grandes bases de données de l'IGN, dès le 1er janvier 2021. En effet, la Cour des comptes avait relevé les tensions entre l'injonction faite à l'opérateur de développer ses ressources propres par la commercialisation de ses données et l'obligation légale de les diffuser gratuitement, soulignant que les recettes de vente de données brutes étaient passées de 36 % du chiffre d'affaires de l'IGN en 2013 à seulement 12 % en 2017[484].

Le deuxième modèle identifié par Johnson et Scassa est celui dans lequel l'État conserve la souveraineté sur les données, mais délègue contractuellement tout ou partie de leur production à des prestataires privés[485]. Dans ce cadre, les pouvoirs publics définissent précisément les données à produire et les standards de qualité applicables, tout en confiant l'exécution opérationnelle à des tiers sélectionnés par voie de marchés publics. Le droit de propriété sur les données produites revient en

---

480 Mills Meghan et de Rijcke Izaak, « Geomatics and the law geospatial data: Balancing private ownership and public interest », Geomatica, n°70, 2016, pp. 5-149.

481 Florini A., et Dehqanzada Y., « Commercial satellite imagery comes of age », Issues in Science and Technology, n°16, 1999, pp. 45-52.

482 Supreme Court of Canada, « Keatley Surveying Ltd. v. Teranet Inc », 26 septembre 2019. https://www.scc-csc.ca/judgments-jugements/cb/2019/37863/

483 Khanal Kshitiz, Budhathoki Nama Raj, et Erbstein Nancy, « Filling OpenStreetMap data gaps in rural Nepal: A digital youth internship and leadership programme », Open Geospatial Data, Software and Standards, n°4, 2019, pp. 1-10.

484 Cour des comptes, Référé S2018-3287 sur la valorisation des données de l'IGN, de Météo-France et du Cerema, 11 mars 2019.https://www.ccomptes.fr/sites/default/files/2019-03/20190311-refere-S2018-3287-valorisation-donnees-IGN-Meteo-France-Cerema-rep-PM.pdf. Consulté le 15 mars 2023.

485 Zook Matthew, Graham Mark, Shelton Taylor et Gorman Sean, « Volunteered geographic information and crowdsourcing disaster relief: A case study of the Haitian earthquake », World Medical & Health Policy, n°2, 2012, pp. 6-32.

règle générale à l'administration contractante[486]. En France, ce modèle se retrouve dans le contrat d'objectifs et de performance de l'IGN pour la période 2020-2024, qui prévoit le recours à des partenariats avec des acteurs privés pour la production de certains référentiels, tout en réaffirmant le rôle de l'institut comme opérateur interministériel unique en matière de données géographiques souveraines.

Dans le troisième modèle distingué par Johnson et Scassa, le gouvernement adopte une posture d'acheteur ou d'agrégateur de données, en combinant des jeux de données acquis auprès de producteurs privés avec des sources publiques existantes[487]. Ainsi, à la différence du modèle précédent, l'État s'insère ici dans un marché où les données sont produites selon la logique propre des prestataires et proposées à une multiplicité d'utilisateurs. La disponibilité croissante de l'imagerie satellitaire du secteur privé illustre bien cet enjeu[488], en ce qu'elle fragilise la capacité d'accès exclusif des États à l'information territoriale. La décision Keatley Surveying c. Teranet rendue par la Cour suprême du Canada en 2019 illustre les ressorts juridiques par lesquels un État peut tenter de préserver sa souveraineté dans ce type de configuration[489]. En jugeant que la loi ontarienne faisait du gouvernement le titulaire du droit d'auteur sur les plans d'arpentage déposés au registre foncier provincial, la Cour a consacré un mécanisme de transfert légal de la propriété intellectuelle permettant à l'État de conserver le contrôle sur une base de données produite pour l'essentiel par des opérateurs privés.

Le quatrième modèle enfin, celui que Johnson et Scassa identifient comme la forme la plus avancée de désengagement étatique, correspond à une situation dans laquelle l'État se dessaisit de sa fonction de producteur et d'organisateur des données géographiques au profit d'acteurs non gouvernementaux[490]. Ce scénario a néanmoins trouvé des applications concrètes dans des contextes de crise. Ainsi, lors du séisme qui a frappé Haïti en 2010, les équipes d'intervention humanitaire ont dû pallier l'absence quasi totale de données géospatiales gouvernementales disponibles en recourant aux données en accès libre de la plateforme OpenStreetMap[491], ainsi qu'aux images satellitaires privées

---

[486] Sieber Renee E., et Johnson Peter A., « Civic open data at a crossroads: Dominant models and current challenges », Government Information Quarterly, n°32, 2015, pp. 308-315.

[487] Elwood Sarah, « Grassroots groups as stakeholders in spatial data infrastructures: Challenges and opportunities for local data development and sharing », International Journal of Geographical Information Science, n°22, 2008, pp. 71-90.

[488] Scassa Teresa, « Law enforcement in the age of big data and surveillance intermediaries: Transparency challenges », SCRIPT-Ed, n°14, 2017, pp. 239-284.

[489] Ibid.

[490] Couture Stéphane et Toupin Sophie, « What does the notion of "sovereignty" mean when referring to the digital? », New Media & Society, n°21 (10), 2019, pp. 2305-2322. https://doi.org/10.1177/1461444819865984

[491] Roberts Huw et alii, « Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models », Digital Society, Springer Nature, 2024. https://link.springer.com/article/10.1007/s44206-024-00146-7

fournies par Google et GeoEye[492]. Ces deux exemples démontrent l'impact d'un manque d'infrastructure de données spatiales au niveau gouvernemental. En conséquence, d'autres sources de données spatiales ont été adoptées au moins en partie, et le gouvernement s'est retrouvé dans le rôle d'utilisateur final ou de destinataire plutôt que de créateur de données. Pour les gouvernements qui ont déjà entretenu une infrastructure de données spatiales, un retrait de la collecte de données entraîne l'abandon du contrôle non seulement de la propriété, mais aussi de l'utilisation qui peut en être faite, ainsi que des capacités techniques ou institutionnelles de saisie et de traitement des données géographiques. Des tiers pourraient dès lors vendre ou concéder sous licence des données spatiales pour une multiplicité d'usages, y compris ceux qui seraient contraires au bien public, soulevant des questions de responsabilité juridique et de transparence que le droit peine à trancher dans ce type de configuration

Aujourd'hui, le gouvernement français fonctionne selon le deuxième modèle, où la production et la collecte de données géographiques sont principalement sous la responsabilité d'agences gouvernementales, comme l'IGN. La participation d'acteurs privés à la collecte et à l'exploitation de certaines données n'est pas exclue. Cependant, avec l'évolution du mode de financement de l'IGN et la diminution des subventions publiques qui lui sont octroyées, il n'est pas exclu de voir l'État français évoluer vers d'autres modes de production et de diffusion des données géographiques. Cette évolution n'est pas nécessairement problématique en soi, mais elle suppose que des garde-fous contractuels et réglementaires solides soient mis en place pour éviter que le glissement vers un modèle d'agrégateur de données privées ne se fasse au détriment de la souveraineté de l'État sur les référentiels géographiques qui fondent ses politiques publiques. La question du maintien de la souveraineté de l'État sur les données qui seraient alors produites pose question. Il est donc nécessaire de chercher à évaluer les différents mécanismes de conservation ou de transfert de la souveraineté des États dans le domaine de la production de données géographiques.

[492] Johnson Peter A. et Scassa Teresa, « Who owns the map? Data sovereignty and government spatial data collection, use, and dissemination », Transactions in GIS, n° 27, 2023, pp. 275–296. https://onlinelibrary.wiley.com/doi/abs/10.1111/tgis.13024

2.3 Quelles évolutions concernant la souveraineté des données géographiques ?

Ainsi, si la France opère aujourd'hui selon un modèle de délégation encadrée, la tendance à l'érosion des subventions publiques aux opérateurs nationaux, conjuguée à la montée en puissance des acteurs privés du numérique dans la production de données géographiques, soulève une question pratique. Quels mécanismes concrets permettent aux gouvernements de conserver ou, au contraire, de céder leur souveraineté sur ces données ? Cette question, qui dépasse le seul cadre français, a fait l'objet d'un traitement approfondi dans la littérature anglophone relative aux infrastructures de données spatiales. Les travaux de Johnson et Scassa (2023) identifient notamment trois mécanismes structurants : le financement public pérenne, la contractualisation encadrée avec le secteur privé, et le recours au droit d'auteur de l'État comme instrument de contrôle [493]. Il convient toutefois d'évaluer la portée de ces mécanismes à l'aune des évolutions propres au contexte européen et français, où la politique d'ouverture des données publiques a profondément recomposé les rapports de force entre État, collectivités et opérateurs tiers.

La dimension budgétaire constitue sans conteste le fondement de tout régime de souveraineté sur les données. En effet, la capacité des pouvoirs publics à assurer la collecte, la mise à jour et la diffusion de données géographiques de référence est directement conditionnée par les ressources humaines et financières consacrées à ces tâches. La littérature a bien documenté cette dépendance, en soulignant que les fonctions clés assurées par les administrations, (infrastructure, archivage, diffusion), ne peuvent être déléguées sans risque de perte de compétence interne [494]. Ce constat revêt une acuité particulière dans des pays où les données géographiques officielles jouent un rôle clé dans l'élaboration des politiques publiques, notamment en matière d'aménagement du territoire, de prévention des risques ou de protection des populations les plus vulnérables [495]. Or la trajectoire financière de l'IGN illustre précisément les risques induits par une réduction progressive des dotations publiques. La Cour des

---

493 Johnson Peter A. et Scassa Teresa, « Who owns the map? Data sovereignty and government spatial data collection, use, and dissemination », Transactions in GIS, n° 27, 2023, pp. 275–296. https://onlinelibrary.wiley.com/doi/abs/10.1111/tgis.13024

494 Sieber Renee E. et Johnson Peter A., « Civic open data at a crossroads : Dominant models and current challenges », Government Information Quarterly, n° 32, 2015, pp. 308–315.https://www.researchgate.net/publication/278161820_Civic_open_data_at_a_crossroads_Dominant_models_and_current_challenges

495 Elwood Sarah, « Grassroots groups as stakeholders in spatial data infrastructures : Challenges and opportunities for local data development and sharing », International Journal of Geographical Information Science, n° 22, 2008, pp. 71–90.https://www.tandfonline.com/doi/abs/10.1080/13658810701348971

comptes avait relevé dès 2019 que les recettes commerciales de l'établissement, qui représentaient 36 % de son chiffre d'affaires en 2013, étaient tombées à 12 % en 2017, traduisant l'incapacité croissante de l'opérateur à valoriser commercialement ses productions face à la concurrence des plateformes privées. La décision d'ouvrir gratuitement l'ensemble des bases de données de l'IGN à compter du 1er janvier 2021 règle cette contradiction, mais elle reporte intégralement le financement de la production de données souveraines sur la subvention étatique. Si cette dernière venait à être réduite, c'est la capacité même de l'État à produire des référentiels faisant autorité qui se trouverait compromis.

Face à cette contrainte budgétaire, la tentation est grande pour les gouvernements de s'appuyer sur des acteurs privés pour assurer tout ou partie de la production de données géographiques. Cette stratégie n'est pas dénuée d'intérêt. Ainsi, dans des zones rurales ou éloignées où le maillage des services publics est insuffisant, l'intégration de prestataires tiers dans la chaîne de collecte de données permet d'étendre la couverture territoriale à moindre coût. Ainsi, des initiatives comme le projet Global ML Building Footprint de Microsoft, lancé en 2022 pour mettre à disposition des gouvernements des données d'empreintes de bâtiments produites par analyse d'imagerie satellitaire, incarnent ce modèle de partenariat [496]. Malgré des exemples positifs, il existe des cas où des données gouvernementales ont été fournies en tant que données ouvertes, puis utilisées d'une manière qui n'était pas conforme à l'intention initiale du gouvernement. Ainsi, la ville de Toronto au Canada a fourni en 2011 des données sur la criminalité à des plateformes de cartographie américaines, notamment Central Square Technologies via sa plateforme CrimeMapping.com, plutôt que de créer ses propres cartes ou de fournir ces données dans des formats ouverts, ce qui fait que les données concernant la criminalité y sont aujourd'hui représentées d'une façon similaire aux données américaines[497]. Cela démontre une perte de souveraineté résultant d'une relation de partage de données imprécise qui a lié des données gouvernementales à des plateformes du secteur privé.[498]

Au-delà de la question contractuelle, le droit d'auteur de l'État constitue un troisième levier souvent sous-estimé dans le débat sur la souveraineté des données géographiques. Nombre de juridictions reconnaissent que l'État est titulaire du droit d'auteur sur les œuvres créées ou publiées sous sa direction ou son contrôle. Si la Convention de Berne se borne à viser les *« textes officiels de nature législative, administrative et juridique »* [499], cette protection peut s'étendre, selon les systèmes nationaux, aux cartes et aux bases de données qui en constituent la traduction cartographique. Or, en

---

496 Voir à ce sujet : https://github.com/microsoft/GlobalMLBuildingFootprints

497 Scassa Teresa, « Law enforcement in the age of big data and surveillance intermediaries: Transparency challenges », SCRIPT-Ed, n° 14, 2017, pp. 239–284. https://www.researchgate.net/publication/321823204_Law_Enforcement_in_the_Age_of_Big_Data_and_Surveillance_Intermediaries_Transparency_Challenges

498 Organisation mondiale de la propriété intellectuelle (OMPI), « Convention de Berne pour la protection des œuvres littéraires et artistiques », Introduction, 28 septembre 1979.

499 Ibid.

matière de données géographiques, la protection par le droit d'auteur de l'État joue historiquement un double rôle, elle garantit d'abord l'intégrité et l'authenticité des textes officiels [500], mais elle sert également d'instrument de contrôle sur la reproduction et la commercialisation des données géographiques [501]. Cette dualité est particulièrement visible dans les arbitrages qui entourent les politiques d'ouverture des données. En effet, si la logique de l'open data conduit à une mise à disposition sans restriction technique, juridique ou financière significative [502], elle implique cependant de la part de l'État une décision consciente d'exercer son droit de propriété sur les données pour les libérer, et non de l'abandonner. La distinction est capitale. Dans le premier cas, l'État demeure souverain et fait un choix de politique publique et dans le second, il cède son contrôle à des tiers dont les objectifs peuvent être étrangers à l'intérêt général. C'est précisément ce glissement que la décision Keatley Surveying c. Teranet rendue par la Cour suprême du Canada en 2019, déjà mentionnée, cherchait à prévenir en consolidant la propriété étatique sur les données issues de l'enregistrement foncier.

La mise en perspective de ces trois mécanismes avec la situation française révèle une tension structurelle qui n'a pas encore été complètement résolue. D'un côté, la France a fait le choix d'une ouverture massive de ses données géographiques, en libérant les bases de l'IGN sous licence ouverte et en développant des standards nationaux via le CNIG pour en favoriser la réutilisation. Cette décision, pleinement justifiée au regard des objectifs de transparence et de démocratisation de l'information, a simultanément affaibli les deux premiers mécanismes de souveraineté. Elle a supprimé la source de revenus commerciaux qui contribuait au financement de l'opérateur public, et elle a élargi considérablement l'espace d'exploitation de ces données par des acteurs privés dont les usages sont difficilement contrôlables. De l'autre, le troisième mécanisme, celui du droit d'auteur de l'État, demeure théoriquement disponible mais son exercice effectif suppose une vigilance juridique et technique que les administrations françaises, dont la gestion des données géographiques est éclatée entre de multiples opérateurs et collectivités, ne peuvent pas toujours garantir. De fait, la souveraineté sur les données géographiques n'est pas un état stable. Elle est le résultat d'un effort continu, budgétaire, contractuel et juridique, dont l'interruption, même partielle, ouvre des brèches que les acteurs privés sont prompts à combler.

---

500 Johnson Peter A., « Models of direct editing of government spatial data : Challenges and constraints to the acceptance of contributed data », Cartography and Geographic Information Science, vol. 44, 2017, pp. 128–138.https://www.tandfonline.com/doi/full/10.1080/15230406.2016.1176536

501 Mills Megane et de Rijcke Izaak, « Geomatics and the law — geospatial data : Balancing private ownership and public interest », Geomatica, vol. 70, 2016, pp. 5–149.

502 Kummitha Rama Krishna Reddy, « Smart technologies for fighting pandemics : The techno- and human-driven approaches in controlling the virus transmission », Government Information Quarterly, vol. 37, 2020.

Les travaux les plus récents sur la gouvernance des infrastructures de données numériques soulignent généralement les gains inhérents à l'ouverture des données. Qu'il s'agisse de l'accélération de l'innovation dans les secteurs public et privé, de l'amélioration de la participation citoyenne, ou encore de la réduction des asymétries d'information entre administrations et administrés[503]. Certains chercheurs ont même proposé le concept d'« infrastructure de données ouverte », dans laquelle gouvernements, secteur privé et citoyens contribuent collectivement à la production d'un commun informationnel[504], rejoignant les réflexions développées dans le domaine des villes intelligentes sur la valorisation des données comme bien commun[505]. Cependant, la transposition de ce modèle au domaine des données géographiques se heurte à une contrainte spécifique, contrairement à de nombreuses autres catégories de données publiques, les données géographiques sont liées à l'exercice de prérogatives régaliennes (définition des frontières, gestion du cadastre, prévention des risques naturels) dont la délégation ne saurait être totale sans mettre en cause les fondements de la souveraineté territoriale. Ainsi, si la libéralisation des données géographiques contribue à enrichir l'écosystème numérique national, elle crée simultanément des canaux de dépendance vis-à-vis d'acteurs dont les logiques de valorisation peuvent diverger substantiellement des intérêts de l'État. La tension entre ouverture et souveraineté ne peut donc pas trouver sa solution uniquement au niveau de la politique des données. Elle suppose une réflexion élargie sur les conditions dans lesquelles l'État peut maintenir sa capacité d'action sans renoncer aux bénéfices de l'interopérabilité et du partage.

C'est précisément à cette jonction que se trouve les enjeux de la normalisation. En effet, les normes constituent l'un des rares instruments techniques à même de concilier les exigences contradictoires d'ouverture et de contrôle. En définissant les conditions d'interopérabilité des systèmes, elles permettent à l'État de maintenir une capacité de surveillance et de validation sur des données dont il n'est plus nécessairement le seul producteur. Or cette vocation régulatrice des normes géographiques se heurte aujourd'hui à un défi important, celui de la protéger contre des attaques informatiques dont les cibles et les effets sont de plus en plus précisément calculés. La mise en réseau des données géographiques, condition de leur utilisabilité et de leur diffusion, en fait simultanément des cibles potentielles dont le piratage et la falsification pourraient avoir des conséquences graves sur la capacité

---

503 Beckwith Richard, Sherry John et Prendergast David, « Data flow in the Smart City : Open data versus the commons », in M. de Lange et M. de Waal (dir.), The Hackable City, Springer, 2019, pp. 205–221.https://link.springer.com/chapter/10.1007/978-981-13-2694-3_11

504 Vancauwenberghe G., Valėčkaitė K., Van Loenen B. et Donker F., « Assessing the openness of spatial data infrastructures (SDI) : Towards a map of open SDI », International Journal of Spatial Data Infrastructures Research, n° 13, 2018, pp. 88–100.https://www.researchgate.net/publication/323521479_Assessing_the_Openness_of_Spatial_Data_Infrastructures_SDI_Towards_a_Map_of_Open_SDI

505 Johnson Peter A. et Scassa Teresa, « Who owns the map? Data sovereignty and government spatial data collection, use, and dissemination », Transactions in GIS, n° 27, 2023, pp. 275–296.https://onlinelibrary.wiley.com/doi/abs/10.1111/tgis.13024

de l'État à gérer son territoire et à assurer la sécurité de ses citoyens. C'est l'examen de cette menace, et des premières réponses normatives qui sont développés, qui constitue l'objet de la section suivante.

3. La mise en place par de premières mesures en matière de protection de données géographiques pour les forces armées

L'implémentation de mesures de sécurité au sein même du processus de développement des normes en matière d'information géographique ne va pas de soi. En effet, le but premier des normes est avant tout d'assurer l'interopérabilité de différents éléments. Cette injonction, qui est au cœur même de la création de normes, s'oppose en principe aux exigences de la cybersécurité qui imposent de mettre des barrières à l'échange d'information afin de pouvoir contrôler qui a accès à quelles informations. De plus, le souci légitime de mettre à la disposition du plus grand nombre un maximum d'informations géographiques tend à reléguer au second plan les problématiques de cybersécurité au sein de la communauté de la géomatique. Cependant, avec l'augmentation radicale des cyberattaques, il convient de plus en plus d'assurer la transformation des architectures de données géographiques afin de garantir la protection des données qu'elles contiennent. La transformation de ces plateformes doit se faire de manière à garantir la fourniture et l'utilisation sûres et sécurisées des services numériques afin de protéger les informations et la vie privée des citoyens. L'ouverture de l'architecture et l'adoption de nouvelles technologies peuvent rendre les appareils et les données vulnérables à des atteintes malveillantes ou accidentelles à la sécurité et à la confidentialité. Les architectures doivent adopter des solutions dans des domaines tels que la surveillance continue, la gestion des identités, de l'authentification et des références, et la cryptographie, qui permettent de passer de la sécurisation des appareils à la sécurisation des données elles-mêmes et qui garantissent que les données ne sont partagées qu'avec les utilisateurs autorisés. Bien qu'initialement développée pour répondre aux besoins civils et institutionnels en matière de gestion des données géographiques, l'injection de mesures de cybersécurité dans des normes géographiques trouve également des applications critiques dans des contextes militaires. En effet, avec l'évolution technologique et l'intégration croissante de capteurs et de réseaux numériques dans les forces armées, la cybersécurité des données géospatiales est devenue un enjeu stratégique majeur. Cependant, l'intégration de mesures de cybersécurité dans les normes militaires fait encore face à un certain nombre de défis.

3.1 Le domaine militaire et l'importance de la prise en compte du risque cyber dans la normalisation

Grâce au déploiement de capteurs de données géographiques au service des armées et à leur interconnexion accrue au cours de la décennie 2010, la cybersécurité de ces réseaux est devenue un enjeu crucial des conflits actuels et à venir. La guerre en Ukraine a démontré les dommages conséquents que pouvait engendrer le piratage d'applications et de logiciels militaires reposant sur l'exploitation de données géographiques, comme les applications de contrôle de tir d'artillerie[506]. Ainsi, la guerre russo-ukrainienne a été le théâtre de multiples cyberattaques ciblant les systèmes d'information géographique militaires. Le cas du système de ciblage GIS Arta en est un bon exemple. Le système GIS Arta (Geographic Information System Art for Artillery), développé par des programmeurs ukrainiens avec la participation d'entreprises britanniques de cartographie numérique, illustre parfaitement les enjeux de cybersécurité des systèmes d'information géographique militaires[507]. Qualifié d'« Uber de l'artillerie », ce logiciel tisse un réseau reliant capteurs, cibles et unités d'artillerie pour assigner automatiquement des missions de tir. Il exploite les données de drones de reconnaissance, de télémètres, de radars et de smartphones pour calculer des solutions de tir optimales en fonction du type de cible, de sa position et de la portée des pièces disponibles, réduisant le temps entre la détection d'un objectif et l'ouverture du feu de vingt minutes à moins d'une minute[508]. Les utilisateurs se connectent au système via téléphones, tablettes ou ordinateurs portables reliés au réseau satellitaire Starlink.

L'efficacité opérationnelle de GIS Arta, crédité notamment de la destruction d'un bataillon russe entier en mai 2022[509], en a fait une cible prioritaire pour les cyberforces russes. De multiples tentatives de piratage ont été menées contre ce système, tant durant le conflit du Donbass (2014-2021) qu'après l'invasion de février 2022, sans succès durable. La résilience du système s'explique par plusieurs facteurs. Tout d'abord, un chiffrement renforcé, mais également la réactivité de l'« IT Army » ukrainienne pour contrer les menaces, et enfin l'architecture décentralisée du réseau qui complique les attaques ciblées[510].

---

506 The Economist, « Why are so many Russian generals dying in Ukraine? », 31 mars 2022. ; Lorenzo Franceschi-Bicchierai, « Fancy Bear Hack of Ukrainian Artillery Fighters Shows Future of War », Vice, 22 decembre 2016.

507 HandWiki, « Software: GIS Arta », 7 mars 2023 ; Charlie Parker, « Uber-style technology helped Ukraine to destroy Russian battalion », The Times, mai 2022.

508 Global Defence Technology, « How radars, reconnaissance and software are shaping the artillery war in Ukraine », juin 2022 ; New America Foundation, « How Ukraine's "Uber for Artillery" is Leading the Software War Against Russia », 2023.

509 The Times, « Uber-style technology helped Ukraine to destroy Russian battalion », mai 2022.

510 Lviv Herald, « A Forensic Examination of GIS Arta », 6 juillet 2025 : « Russian forces have tried repeatedly to compromise GIS Arta through cyberattacks and electronic warfare, but without lasting success—due to both hardened encryption and the agility of Ukraine's IT Army in countering threats ».

Face à l'échec des cyberattaques directes, la Russie a développé des approches alternatives pour neutraliser l'avantage informationnel ukrainien. Dès janvier 2023, la société russe de technologie militaire VPK documentait l'utilisation par les soldats russes d'applications de triangulation acoustique sur smartphones pour localiser les positions d'artillerie ukrainiennes[511]. De petites équipes équipées de smartphones ou tablettes se dispersent à quelques kilomètres derrière la ligne de contact et utilisent une application détectant la signature acoustique des tirs d'artillerie. Les données sont transmises à un système central qui triangule la position du canon, confirmée ensuite par drone avant d'être ciblée par des tirs de contre-batterie[512]. Cette technique ancienne, (la télémétrie acoustique existe depuis la Première Guerre mondiale), a ainsi été démocratisée grâce aux smartphones, repoussant la capacité de localisation jusqu'aux échelons tactiques les plus bas. Parallèlement, les forces russes ont intensifié leur guerre électronique contre les systèmes de guidage GPS dont dépendent GIS Arta et les munitions de précision occidentales. Le brouillage des signaux GPS a drastiquement réduit l'efficacité des obus Excalibur guidés par satellite, passée de 70% à moins de 10% après le déploiement des contre-mesures russes[513]. Cette dégradation des capacités de géolocalisation affecte l'ensemble de la chaîne de ciblage ukrainienne, depuis la reconnaissance jusqu'à la frappe. Ces attaques montrent combien l'exploitation malveillante des données de localisation et de cartographie peut influencer le cours des combats. À titre d'exemple, pour compenser son infériorité en artillerie, l'Ukraine utilise depuis 2018 une application mobile baptisée Kropyva (système cartographique tactique) pour coordonner avec précision les tirs de ses canons, en liaison avec des drones d'observation. En raison de son efficacité à infliger des dégâts à l'ennemi, Kropyva est devenue une cible pour les hackers russes. Le groupe Fancy Bear a notamment lancé des attaques sur les hubs de connexion satellite utilisés par l'application, dès le début de l'invasion en 2022, dans le but de perturber les communications et l'échange de données de ciblage[514]. Cette tentative de neutralisation a été déjouée grâce à l'utilisation du réseau satellite Starlink de SpaceX, qui a pris le relais et assuré la continuité du service. Cet exemple illustre ainsi la nécessité de protections robustes des liaisons de données. Sans alternative résiliente, une armée peut voir ses outils de ciblage high-tech rendus inopérants par une attaque. Si aujourd'hui les armées françaises s'appuient sur des réseaux fermés pour déployer et exploiter les données géographiques disponibles sur les

---

511 Army Technology, « Radars, reconnaissance and software are shaping the artillery war in Ukraine », 10 juin 2022 : « multiple failed attempts were made to hack this program both during the Donbas conflict and after the 2022 invasion ».

512 Lviv Herald, « A Forensic Examination of GIS Arta », 6 juillet 2025 : « Russian forces have tried repeatedly to compromise GIS Arta through cyberattacks and electronic warfare, but without lasting success—due to both hardened encryption and the agility of Ukraine's IT Army in countering threats »

513 Army Recognition, « GPS Jamming key of Russian operational capacities in Ukraine », 2024 ; témoignage devant la Chambre des représentants des États-Unis, mars 2024.

514 Sylvain Biget, « Guerre en Ukraine : Kropyva, l'application Android utilisée par les artilleurs ukrainiens », Futura-Science, 2022. https://www.futura-sciences.com/tech/actualites/guerre-futur-guerre-ukraine-kropyva-application-android-utilisee-artilleurs-ukrainiens-99045/

différents théâtres d'opérations, le développement de programmes, comme GEODE 4D ou le programme Scorpion (via le SICS), va changer la donne. De plus en plus, la numérisation et la robotisation des armées pousse au développement de réseaux interconnectés entre les différentes unités et échelons et, par la même occasion, à la diffusion de données géographiques à travers des flux qu'il est nécessaire de pouvoir protéger. La fiabilité des données ainsi diffusées est capitale dans un contexte militaire où des décisions impliquant la vie et la mort peuvent reposer sur des analyses terrain que l'on souhaite toujours plus précises et détaillées.

Jusque dans les années 1990, la majorité des données géographiques numériques militaires étaient produites dans des formats propriétaires extrêmement restrictifs ne pouvant généralement être consultés que sur des systèmes d'exploitation militaires propriétaires. En effet, jusqu'à la fin de la guerre froide, du fait des besoins très spécifiques requis par les systèmes d'armes des armées, que les formats grand public ne pouvaient satisfaire, la majorité des données géographiques étaient produites pour les armées par des sociétés privées spécialisées. Ces dernières fournissant les données à travers des formats propriétaires entièrement sous leur contrôle. Cette situation de quasi-monopole forçait les armées à débourser plusieurs milliers de francs pour rajouter des données à n'importe quel système de préparation de missions [515]. Cette situation engendrait un véritable marketing croisé ou les sociétés privées profitaient de ce manque de flexibilité des données pour facturer aux armées françaises le moindre changement dans les données. Si une telle situation garantissait indirectement une solide protection contre une éventuelle perte ou modification de données, du fait de l'extrême impraticabilité de ces dernières (impossible de les visualiser en dehors des systèmes d'information militaires de l'armée française), leur manque de flexibilité catastrophique nécessitait une évolution. Un travail d'envergure a donc été entrepris à partir de la fin des années 1990 afin de normaliser les formats de données utilisées pour fluidifier leur production et leur échange, brisant du même coup le monopole de ces sociétés privées. Les premières normes en matière de données militaires ont progressivement évolué vers plus de flexibilité et d'ouverture, passant de formats spécifiques, comme le VMAP [516], vers des modèles comme le DTED[517] et ceux employés dans le programme MGCP, qui contient des fichiers Shapefile grand public développés par Esri et exploitables par n'importe quel système d'information géographique. Avec le développement de groupes de travail sur les normes ouvertes en matière de

---

515 Entretien avec le directeur de la société Géo212, 23 février 2022.

516 Vector Map (VMAP), est une collection de données géospatiales vecteurs sur la Terre, disponible à différents niveaux de détail. Le VMAP Niveau 0 (VMAP0) offre une couverture mondiale à petite échelle (1 : 1 000 000) et est structuré selon le Vector Product Format (VPF), conforme aux normes MIL-V-89039 et MIL-STD 2407 adoptées par l'armée américaine. Source : https://web.archive.org/web/20060425195310/http://www.nga.mil/portal/site/nga01/index.jsp?epi-content=GENERIC&itemID=a2986591e1b3af00VgnVCMServer23727a95RCRD&beanID=1629630080&viewID=Article

517 Digital Terrain Elevation Data (DTED) est un format standard pour les données d'élévation numérique, largement utilisé dans les applications militaires pour représenter la topographie du terrain.

données géographiques pour les armées, comme le DGIWG, et le développement de programmes de coproductions et de STANAGs OTAN, les normes employées au sein des armées françaises ont progressivement évolué. De normes très spécifiques développées dans les années 1990 pour fluidifier la production de données géographiques au sein des armées françaises, ces dernières sont passées à des normes fondées sur des normes civiles grand public, en particulier sur celles de l'OGC. Ce souci d'interopérabilité élevé à une échelle internationale a été un moteur de cette transformation qui a amené les armées à adopter des modèles de données plus grand public. Cependant, ce que ces données ont gagné en flexibilité, elles l'ont perdu en protection en devenant plus faciles à étudier et à manipuler. Le renforcement de leur mise en réseau expose d'autant plus les systèmes d'informations géographiques militaires à des attaques cybernétiques. D'aucuns diraient qu'une telle situation doit amener avant tout au renforcement des compétences des armées en matière de cybersécurité par le recrutement et l'entraînement de plus de spécialistes en cyber aptes à protéger les systèmes d'information existants et futurs. Cependant, la normalisation peut ici tirer son épingle du jeu en facilitant le développement de mesures de sécurité au cœur même des normes. Cela contribue également à renforcer la résilience cyber des systèmes « à la base », c'est-à-dire dès la conception des formats de données.

3.2 Le DGIWG et la cybersécurité : comment marier sécurité et normes ouvertes ?

Il apparaît évident aujourd'hui que les enjeux liés à la cybersécurité ne sont pas des préoccupations de premier plan pour les organisations de normalisation, comme le DGIWG. Ainsi, pris en quelque sorte entre l'enclume de l'interopérabilité et le marteau de l'ouverture, la cybersécurité se trouve reléguée au second plan, ou purement et simplement ignorée dans les normes du DGIWG. En effet, la plupart des experts en normalisation n'ont pas d'expérience en matière de cybersécurité, et considèrent généralement que ces problématiques sont du ressort des informaticiens de chaque nation qui ont en charge de protéger leurs différents systèmes d'information tout en les rendant interopérables. De fait, au sein de l'OTAN, les exercices CWIX (Coalition Warrior Interoperability Exercise)[518], couplés aux exercices Locked Shields[519] et Crossed Swords[520] organisés par le Centre d'excellence de cyberdéfense coopérative (CCDCOE) de Tallinn, se chargent de renforcer les capacités cyber de l'Alliance atlantique tout en garantissant l'interopérabilité des systèmes développés par les nations alliées. Cette situation renforce donc au sein des communautés d'experts en normalisation le sentiment que ces questions sont en dehors de leur juridiction. Néanmoins, au sein d'un système d'information, ce sont bien les normes qui définissent les opérations disponibles ou non aux utilisateurs. Ce sont ces mêmes opérations qui délimitent l'étendue des actions possibles et potentiellement dangereuses si elles étaient employées à mauvais escient. Ainsi, même s'il apparaît évident que les normes ne permettront pas de régler l'ensemble des problèmes liés à l'interconnexion des systèmes militaires ou même civils, ignorer la cybersécurité au sein des instances de normalisation serait une erreur.

Tout d'abord, comme démontré dans un article récemment écrit[521] les normes en matière de données géographiques constituent des architectures interconnectées au sein des systèmes d'information qui les emploient. Ces mêmes architectures normatives peuvent constituer des vecteurs

---

518 CWIX est le principal exercice annuel d'interopérabilité numérique de l'OTAN. Créé en 1999 sous le nom de Joint Warrior Interoperability Demonstration, il a été renommé CWIX en 2009 pour refléter son évolution vers un exercice à part entière. Voir à ce sujjet : NATO Allied Command Transformation, « CWIX 2024: NATO's Largest-Ever Digital Interoperability Exercise Concludes », 21 juin 2024 ; NATO ACT, « 25 Years of CWIX: Largest-Ever Interoperability Exercise Kicks Off », 3 juin 2024 ; NATO JFTC, « Coalition Warrior Interoperability Exercise – the Gold Standard for Assuring Digital Interoperability », 20 juin 2025

519 Organisé par le NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) depuis 2010, Locked Shields est le plus grand exercice de cyberdéfense en temps réel au monde. Il s'agit d'un exercice Red Team vs Blue Team où des équipes nationales défendent des systèmes informatiques simulés contre des cyberattaques en direct. Voit à ce sujet : NATO CCDCOE, « World's largest cyber defense exercise Locked Shields kicks off in Tallinn », 2023 ; NATO ACT, « Cooperative Cyber Defence Centre of Excellence: Locked Shields Exercise Showcased the Power of Cooperative Defence », 28 juillet 2024 ; NATO, « NATO Allies and partners participate in large-scale cyber defence exercise », 19 avril 2022.

520 Exercice technique de red teaming organisé annuellement par le CCDCOE depuis 2014, Crossed Swords se concentre sur les opérations cyber offensives et leur intégration avec les opérations cinétiques. Il complète Locked Shields en formant les spécialistes aux capacités offensives.

521 Vigouroux Gauthier, Le Genissel Rémi, Merino Laso Pedro, Claramunt Christophe, et Leidinger Nathalie., « Normative Ecosystem Risk Analysis: Method and Application to OGC Web Services », IEEE, en cours de publication.

d'attaque pour de potentiels attaquants si elles ne sont pas suffisamment protégées, comme démontré par l'article dans le cas des normes OGC. L'absence de protection implémentée dès la constitution des normes pose un risque dès la fondation des systèmes d'information qui nécessitent systématiquement l'intervention d'experts pour sécuriser ces réseaux. Si des mesures de sécurité peuvent être implémentées dès la conception des normes, cela permettrait à terme de proposer une sécurité minimale immédiate aux utilisateurs tout en soulageant le travail des experts en charge de la protection de ces systèmes en aval. Concernant les normes publiées par le DGIWG, la notion de cybersécurité est systématiquement absente. Ainsi, aujourd'hui, seule la norme encore en préparation sur un profil d'implémentation DGIWG de la norme OGC en matière d'EDR[522] (Environmental Data Retrieval) comporte une obligation d'emploi de connexion HTTPS pour l'incorporation des données. L'emploi de HTTPS permet d'ajouter une couche de chiffrement TLS entre l'utilisateur et la source de la donnée et permet à ce dernier de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable (et faisant généralement partie de la liste blanche des navigateurs internet et des systèmes d'exploitation). Il garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans les formulaires) et reçues du serveur. Il peut permettre de valider l'identité du visiteur, si celui-ci utilise également un certificat d'authentification client émis par une autorité fiable. Cela reste cependant une protection assez basique qui demanderait d'être renforcé si l'EDR se retrouve connecté à un ensemble de systèmes d'armes. Le fait que l'existence d'une couche HTTPS ne soit toujours pas imposée par défaut dans l'ensemble des normes du DGIWG démontre l'étendue du manque de prise en compte du risque cyber au sein des organismes de normalisation, même dans un contexte militaire.

De plus, au sein du DGRA, l'architecture normative créée par le DGIWG, des failles de sécurité peuvent être détectées. Ainsi, une présentation à ce sujet a été donnée lors de la réunion technique du 8 avril 2024 démontrant de potentielles failles de sécurité au sein d'un système d'information implémentant les normes du DGRA. En appliquant la même méthode que celle présentée dans l'article publié dans The Cybersecurity Journal à l'architecture normative du DGRA, il a été démontré que certaines normes pouvaient servir de porte d'entrée potentielle pour des attaquants cherchant à modifier ou effacer des données [523]. Aujourd'hui, trouver un juste milieu entre accès, interopérabilité et sécurité reste le défi majeur en matière de cybersécurité dans le domaine de la normalisation. Un dilemme

[522] L'Environmental Data Retrieval (EDR) API est une norme développée par l'Open Geospatial Consortium (OGC) qui propose une série d'interfaces légères pour accéder aux ressources de données environnementales. Elle permet aux utilisateurs de récupérer des données spatio-temporelles en effectuant des requêtes basées sur des positions spécifiques, des zones définies, des trajectoires ou des corridors. Les principales opérations prises en charge par l'API EDR incluent la découverte des capacités du service et la requête de données environnementales selon des critères de sélection simples. Source : https://www.ogc.org/fr/publications/standard/ogcapi-edr/

[523] Le Genissel Rémi et Vigouroux Gauthier, « Analyzing Cybersecurity Risk within a Geographic Standards Ecosystem », DGIWG Technical Panel Meeting, 8 avril 2024.

auquel est confrontée directement l'OTAN dans le développement de ses STANAGs qui se doivent de garantir l'interopérabilité des membres de l'Alliance atlantique tout en garantissant un certain niveau de protection à l'heure où les attaques cyber sont une réalité sur le champ de bataille.

3.3 L'OTAN entre cybersécurité et interopérabilité

La position de l'Alliance Atlantique concernant la cybersécurité reste relativement complexe. L'OTAN considère officiellement le cyberespace comme un domaine de lutte depuis 2016, et a inscrit la cyberdéfense comme une des tâches fondamentales de l'Alliance dans le cadre de la défense collective. Cependant cette défense collective de l'OTAN repose avant tout sur les capacités cyber respectives de chaque État membre [524]. L'OTAN traite officiellement les attaques cyber comme pouvant causer autant de dommages que des attaques traditionnelles. Depuis 2021, l'Alliance Atlantique a mis à jour les conditions entourant une possible application de l'article 5 en indiquant que *« l'impact d'activités cybernétiques cumulatives malveillantes importantes pourrait, dans certaines circonstances, être considéré comme équivalant à une attaque armée »*[525] Cependant, l'OTAN ne communique pas sur ce qui constituerait à ses yeux une attaque cyber d'ampleur similaire à une attaque armée. Dans le même ordre d'idée, l'OTAN ne communique pas sur un « seuil de cybersécurité » commun à l'ensemble des membres de l'Alliance.

La menace cyber semble bien être prise très au sérieux par l'OTAN qui a bâti une solide infrastructure de recherche et de coopération pour répondre aux enjeux de la cybersécurité. Ainsi, l'Alliance dispose du Centre de cybersécurité de l'OTAN (NATO Cyber Security Centre), situé au Grand Quartier général des puissances alliées en Europe à Mons (Belgique), en charge de la protection des réseaux de l'OTAN en apportant un soutien 24 heures sur 24 en matière de cyberdéfense[526]. Ses experts traitent les incidents et fournissent à l'OTAN et aux Alliés une analyse actualisée des menaces cyber. Le NCSC fait partie de l'Agence OTAN de communication et d'information, qui soutient les opérations de l'OTAN, relie les systèmes d'information et de communication des membres de l'Alliance atlantique et défend les réseaux de l'OTAN. L'OTAN a également créé à Mons un centre d'opérations sur le cyberespace. Ce centre permet aux commandants militaires de disposer d'une connaissance de la situation afin d'éclairer les opérations et les missions de l'Alliance. Il est aussi en charge de coordonner également l'activité opérationnelle de l'OTAN dans le cyberespace, en

524 North Atlantic Treaty Organization, « NATO Cyber Defence », Factsheet, avril 2021.

525 Libby Cathey, « How NATO Is Updating Its Common Defense Pact to Deal with Global Cyberattacks », 14 juin 2021, ABC News, https://abcnews.go.com/Politics/nato-updating-common-defense-pact-deal-global-cyberattacks/story?id=78271735.

526 North Atlantic Treaty Organization, « NATO Cyber Defence », Factsheet, avril 2021

garantissant la liberté d'action dans ce domaine et en rendant les opérations plus résistantes aux cybermenaces en cas d'affrontement.

Cette territorialisation de la gouvernance du cyberespace confirme l'intuition d'Yves Lacoste : *« la géographie, ça sert, d'abord, à faire la guerre »* [527], y compris, désormais, la cyberguerre. Loin d'être un espace « aterritorial », le cyberespace se trouve en réalité gouverné depuis des lieux bien précis dont l'ancrage géographique obéit à des logiques de puissance, s'appuyant à la fois sur la mémoire des conflits passés, l'équilibre entre alliés, et la symbolique des espaces frontaliers.

Les opérations dans le cyberespace n'ont cessé de se multiplier ces dernières années et représentent un défi de premier plan pour l'OTAN. Comme le souligne James A. Lewis dans son analyse prospective des opérations cyber à l'horizon 2030, leur caractéristique principale réside dans leur capacité à rester en deçà du seuil d'agression constitutif d'une attaque cinétique, ce qui les rend particulièrement difficiles à encadrer juridiquement et à décourager politiquement[528]. Selon lui, toute règle régissant leur utilisation peut être ignorée en toute sécurité car leur effet est « corrosif », offrant la possibilité d'endommager un adversaire sans engager ses forces militaires, mais l'effet n'est pas si soudain ou violent qu'il justifie des représailles. Les technologies des médias sociaux ouvrent de nouvelles voies à la coercition. La discrétion n'est nécessaire que pour l'insertion, car *« il apparaît de plus en plus que la Russie et la Chine ne se soucient plus d'être prises en flagrant délit »*[529]. Les opérations dans le cyberespace ne remplacent pas l'action cinétique, mais créent *« les effets cognitifs et politiques qui érodent la volonté de résistance de l'adversaire »* [530]. Ainsi, les opérations cyber ne se substituent donc pas à l'action cinétique, elles produisent plutôt *« les effets cognitifs et politiques qui érodent la volonté de résistance de l'adversaire »*[531]. Pour l'Alliance, la différence principale avec les menaces du passé tient, toujours selon Lewis, à ce que les opérations cyber permettent à la fois la violation routinière de la souveraineté, un effet politique accru et l'élargissement des opérations coercitives, cyber et internationales. Cependant, il relève qu'une cyberattaque contre les infrastructures critique ou les systèmes de commandement et de contrôle ne présente pas de risques fondamentalement différents de ceux d'une attaque conventionnelle, ce qui rend la réponse plus facile à planifier[532].

Lewis distingue également les profils stratégiques de chacun des principaux adversaires de l'Alliance dans le cyberespace[533]. Ainsi, il démontre que la guerre en Ukraine a mis au jour l'ampleur

---

[527] Lacoste Yves, *La géographie, ça sert, d'abord, à faire la guerre*, Maspero, 1976.

[528] James A. Lewis, « A Strategic Outlook for Cyberspace Operations », in *Cyberspace Strategic Outlook 2030 Horizon Scanning and Analysis*, NATO CCDCOE Publications, pp. 10–15, 2022.

[529] Ibid

[530] Ibid.

[531] Ibid

[532] Ibid

[533] Ibid.

de la stratégie russe en matière de menace cyber, qui consiste à se préparer à mener des actions extrêmement perturbatrices en cas de conflit, et à poursuivre l'espionnage, les activités politiques et les perturbations mineures dans l'intervalle. Il n'exclut pas que le conflit élargi n'advienne jamais, les difficultés internes de la Russie pouvant freiner l'escalade, mais estime que la planification de l'OTAN doit anticiper des cyberactions russes agressives. Il apparaît indéniable que le seul cout humain et matériel que la guerre en Ukraine impose aujourd'hui à la Russie fait reculer la perspective d'un conflit armée généralisé entre l'OTAN et la Fédération de Russie. Cependant, au même moment, la Chine exerce quant à elle, selon Lewis, une pression économique, informationnelle et cyber croissante sur les pays de l'Alliance, tandis que l'Iran, dont les objectifs diffèrent, reste soumis aux même contraintes. Ainsi, il apparaît aujourd'hui qu'une même réponse peut – être opposé par l'Alliance à ces trois adversaires[534]. L'OTAN se retrouve donc dans une situation particulière où elle doit chercher à « façonner et contraindre leurs actions », ce qui signifie selon Lewis de batir un nouveau cadre conceptuel d'action et un éventail de réponses proportionnées, puis le consensus politique nécessaire pour les employer. Lewis conclut ainsi que *« la défense collective reste le meilleur outil pour protéger la démocratie en contrant les agressions chinoises et russes dans le cyberespace »*[535].

Ce constat sur l'importance de la dimension cyber d'un futur conflit est valable également concernant les systèmes d'informations géographiques, surtout dans l'éventualité d'un conflit de haute intensité. Pour ce faire la protection des données géographiques par l'incorporation de mesures de cybersécurité au sein des normes se doit d'être étudiée par l'OTAN dans la conception de ses systèmes d'informations géographiques. Aujourd'hui, l'OTAN se repose avant tout sur la formation de ses spécialistes en cybersécurité parmi ses pays membres. Le perfectionnement de leurs techniques par le biais des exercices Locked Shields et de l'interopérabilité de leurs systèmes d'information par les exercices CWIX, ce qui fournit à l'OTAN une base solide d'expérimentation et d'entraînement en matière de protection cyber. Cependant, les STANAGs OTAN relatifs aux informations géographiques disponibles publiquement ne semblent pas incorporer de mesures de cybersécurité supplémentaires. Ces derniers se reposent souvent sur des profils DGIWG de normes OGC, parfois modifiés pour s'adapter à des exigences spécifiques. Toujours est-il que, comme pour le DGIWG l'OTAN semble privilégier l'interopérabilité maximale au détriment des mesures de cybersécurité, comme des exigences de cryptographie au sein de ses normes, tout en se reposant sur des mesures prises en aval du processus de construction des systèmes d'information, pour assurer leur protection. Les détails des mesures prises en la matière ne sont bien entendu pas communiqués publiquement pour entretenir le flou sur les capacités cyber de l'OTAN.

[534] Ibid, p. 14
[535] Ibid, p. 15

Ainsi, les données géographiques constituent pour l'État une ressource de premier plan dont il doit garantir la production et la diffusion. La mise en réseau de ces données par l'introduction de services web et de portails de données en ligne nécessite désormais d'incorporer des protections en matière de cybersécurité dans le cycle de production de ces données. La mise a disposition des données géographique restant encore dans la majorité des cas une prérogative de l'État, caractéristique du maintien de sa gouvernance sur son territoire, garantir la protection de ces données est primordial. La multiplication des acteurs privés dans le cycle de production des données, et parfois de leur mise à disposition, comme Google et Microsoft, peut être perçue comme un défi posé à la gouvernance de l'État. Du fait de l'importance de ces données pour la gestion du territoire et, mais également de par leur qualification juridique qui font des données géographiques des données de premières importances pour trancher certains litiges, garantir la qualité et l'authenticité des données est devenu un défi important, à l'heure où de plus en plus d'acteurs se targuent de pouvoir produire et diffuser ces données. Une perte de compétence de l'État concernant les données géographiques pourrait à terme avoir de graves répercussions et rendre les citoyens dépendants d'acteurs non étatiques. La protection de ces données contre les attaques informatiques et les potentielles falsifications qui pourraient en découler est devenue nécessaire. Les organismes de normalisation internationaux prennent de plus en plus conscience de leur rôle crucial dans l'incorporation de mesure de cybersécurité dans les produits contenant des données géographiques, en particulier au sein de certaines communautés, comme la communauté militaire. Cependant, les risques d'attaque cyber concernent en réalité l'ensemble des acteurs en charge de leur production et les conséquences de telles attaques pourraient être handicapantes pour l'ensemble des citoyens qui ont un besoin important d'accès à des informations géographiques de qualité. En France, les infrastructures de données géographiques nationales et régionales permettent aux citoyens de consulter et manipuler des données géographiques de qualité et authentifiées. Ces dernières sont donc en première ligne concernant d'éventuelles attaques cyber et se doivent d'être protégé efficacement, un point qui sera détaillé dans la prochaine partie.

Conclusion du Chapitre IV

Au terme de ce chapitre consacré aux enjeux de la protection des données géographiques contre le risque cyber, plusieurs constats s'imposent qui permettent de dégager les lignes de force d'une géopolitique de la donnée géographique numérique. Il a ainsi pu être démontré que les données géographiques, loin d'être de simples objets techniques neutres, constituent des ressources stratégiques dont la maîtrise engage directement la souveraineté des États. Cette dimension géopolitique, longtemps occultée par une approche purement technique de l'information géographique, apparaît désormais comme un enjeu central des rapports de force contemporains. Trois enseignements majeurs se dégagent du présent chapitre.

Premièrement, la vulnérabilité croissante des données géographiques aux cyberattaques s'inscrit dans un contexte de numérisation accélérée qui transforme profondément les conditions de production, de stockage et de diffusion de l'information spatiale. Les systèmes d'information géographique en ligne, devenus les principaux vecteurs de dissémination des données, constituent autant de surfaces d'attaque potentielles pour des acteurs malveillants. Cette exposition aux risques cyber n'est pas uniforme. Cette dernière varie selon les architectures techniques déployées, les normes implémentées et les moyens consacrés à la sécurisation des infrastructures. Elle dessine ainsi une géographie différenciée de la vulnérabilité, où les territoires les mieux dotés en ressources techniques et humaines se distinguent de ceux qui demeurent exposés faute de moyens adéquats.

De plus, l'examen de la portée juridique des données géographiques a mis en lumière l'articulation étroite entre fiabilité technique et recevabilité légale. Les données géographiques acquièrent une valeur probatoire à proportion de leur intégrité, de leur traçabilité et de l'authenticité de leur source. Dès lors, toute compromission de ces propriétés, qu'elle résulte d'une cyberattaque, d'une erreur de manipulation ou d'une falsification délibérée, menace non seulement l'utilité opérationnelle des données, mais également leur qualification juridique. Cette dimension juridique confère aux enjeux de cybersécurité une portée qui dépasse largement la sphère technique. La normalisation et la diffusion des données géographiques touchent aux fondements mêmes de l'État de droit, dans la mesure où les données géographiques participent de plus en plus à l'établissement des faits dans les procédures administratives et contentieuses. La normalisation des données géographiques apparaît ainsi comme un levier de souveraineté juridique, en ce qu'elle garantit la production de données dont la valeur probatoire peut être reconnue par les juridictions nationales et internationales.

L'analyse des modèles de gouvernance des données géographiques quant à elle, a révélé les tensions qui traversent le champ de la production cartographique contemporaine. La typologie ici exposée, distinguant le modèle étatique pur, le partenariat public-privé encadré, le contrôle partagé et la

délégation intégrale, permet de situer les différentes configurations nationales sur un spectre allant du contrôle souverain maximal à la dépendance vis-à-vis d'acteurs privés transnationaux. Le cas français, qui relève principalement du deuxième modèle, n'est pas à l'abri d'une évolution vers des formes plus hybrides, sous l'effet conjugué des contraintes budgétaires pesant sur les opérateurs publics et de la montée en puissance des acteurs privés du numérique. Ainsi, la souveraineté cartographique loin d'être un acquis définitif, est en réalité une construction politique permanente, tributaire des choix d'investissement et des orientations stratégiques des pouvoirs publics.

L'examen du domaine militaire a confirmé et amplifié ces constats. La guerre en Ukraine a fourni une démonstration grandeur nature de l'importance stratégique des systèmes d'information géographique dans les conflits contemporains. Les tentatives de compromission du système GIS Arta par les forces russes, les attaques contre l'application Kropyva, et plus largement l'intégration du cyberespace comme cinquième domaine de conflictualité par l'OTAN, attestent que la donnée géographique est devenue une arme et, de façon corollaire, une cible. L'analyse de l'architecture institutionnelle de cyberdéfense de l'Alliance atlantique a par ailleurs révélé une géographie singulière, où la localisation des centres d'excellence (Tallinn, Oberammergau, Oeiras, Rome) obéit à des logiques géopolitiques mêlant mémoire des conflits passés, équilibre des puissances et symbolique des frontières. Cette territorialisation de la gouvernance du cyberespace confirme que l'espace numérique, souvent présenté comme « aterritorial », se trouve en réalité gouverné depuis des lieux bien précis, dont l'ancrage spatial constitue une ressource politique à part entière.

Au cœur de ces enjeux, la normalisation apparaît comme un outil ambivalent. D'un côté, les normes de l'OGC et de l'ISO ont permis une interopérabilité sans précédent des systèmes d'information géographique, facilitant l'échange et le partage des données à l'échelle mondiale. De l'autre, cette ouverture a accru la surface d'attaque des infrastructures et complexifié leur sécurisation. Les normes OGC WSS et GeoXACML, développées spécifiquement pour répondre aux impératifs de cybersécurité dans le domaine géospatial, constituent une réponse partielle à ce dilemme. Elles témoignent d'une prise de conscience croissante, au sein des organismes de normalisation, de la nécessité d'intégrer les exigences de sécurité dès la conception des standards, ce que les spécialistes nomment l'approche « security by design ». Toutefois, comme l'a montré l'analyse des normes du DGIWG, cette intégration demeure embryonnaire dans le domaine militaire, où l'impératif d'interopérabilité tend encore à primer sur les considérations de cybersécurité.

Sur le plan théorique, ce chapitre a permis de confirmer la pertinence d'une approche géopolitique du cyberespace, tel que l'a conceptualisée Frédérick Douzet. Le cyberespace, entendu comme *« espace d'information généré par l'interconnexion globale des systèmes d'information et de*

communication »[536], n'abolit pas la géographie, bien au contraire. Il la reconfigure. Les rivalités de pouvoir qui s'y déploient demeurent ancrées dans des territoires, portées par des acteurs situés, et articulées à des représentations spatiales qui orientent les stratégies. La dialectique entre territorialité et réticularité, pour reprendre les catégories de Frédéric Tesson, trouve dans le domaine de la cybersécurité des données géographiques une illustration frappante. Si les menaces circulent dans des réseaux déterritorialisés, les dispositifs de défense, les institutions de gouvernance et les normes qui les encadrent restent, eux, profondément territorialisés.

[536] Douzet, Frédérick. « Le cyberespace, un enjeu majeur de géopolitique », La revue des médias (INA), 1er juillet 2016. [En ligne] URL : https://larevuedesmedias.ina.fr/le-cyberespace-un-enjeu-majeur-de-geopolitique

Chapitre V- Les infrastructures de données géographiques au cœur du risque cyber

Ces constats appellent un changement d'échelle dans l'analyse. Si le chapitre IV a permis d'identifier les enjeux généraux de la protection des données géographiques et d'en esquisser les dimensions juridiques, politiques et militaires, il convient désormais de porter le regard sur les infrastructures concrètes qui assurent la production et la diffusion de ces données. Car les données géographiques n'existent pas dans l'abstraction, elles sont stockées, traitées et mises à disposition par des plateformes numériques dont la sécurisation conditionne directement leur intégrité et leur disponibilité.
C'est donc vers une géographie des infrastructures de données géographiques que cette partie se tourne. Cette géographie est plurielle, et articule l'échelle nationale, où des plateformes comme la Géoplateforme de l'IGN jouent un rôle structurant, l'échelle régionale, où une mosaïque de portails territoriaux assure le maillage du territoire, et l'échelle internationale, où les architectures militaires de l'OTAN et les réseaux civils de l'Union européenne définissent les conditions de l'interopérabilité et de la sécurité. À chacune de ces échelles, les infrastructures de données géographiques constituent des nœuds critiques dont la protection relève désormais d'un impératif de sécurité nationale.
Le chapitre V s'attachera donc à analyser les vulnérabilités spécifiques de ces infrastructures et les politiques publiques mises en œuvre pour y répondre. Il s'agira d'abord d'examiner les responsabilités incombant aux diffuseurs de données géographiques, qu'ils soient publics ou privés, et d'évaluer dans quelle mesure les dispositifs existants permettent d'anticiper et de contrer les risques d'attaques informatiques. Ensuite, il sera présenté comment les normes constituent un outil clé pour développer la résilience des plateformes, en standardisant les bonnes pratiques et en favorisant l'interopérabilité des systèmes de sécurité. L'analyse du rôle du Conseil national de l'information géolocalisée (CNIG) permettra d'éclairer les dynamiques nationales de normalisation et leur articulation avec les instances internationales. Enfin, le cas spécifique des systèmes d'information militaires sera approfondi, à travers l'étude des nouvelles architectures de données numériques déployées par les armées, telles que l'Integrated Sensor Architecture, et des défis qu'elles posent en matière de cyberdéfense.
En portant l'attention sur les infrastructures de données géographiques, le chapitre V permettra ainsi de confronter les ambitions affichées en matière de cybersécurité aux capacités effectives de protection déployée sur le terrain, et d'identifier, le cas échéant, les écarts entre la doctrine et la pratique, entre le prescrit et le réel.

1. Protéger les Infrastructures de données géographiques nationales, une affaire de politiques publiques

La protection des infrastructures de données géographiques sur le territoire français doit donc faire l'objet d'une attention toute particulière afin de garantir la protection des données produites et leur diffusion sans crainte d'interférence auprès de l'ensemble de la population. C'est notamment ce que souligne Makoto Hanashima dans une étude consacrée aux services d'information géographiques des collectivités locales déjà en 2005[537]. En effet, les SIG en ligne constituent aujourd'hui la principale voie d'accès aux données géographiques collectés sur le territoire et employé à des fins de politiques publiques [538]. S'assurer du bon fonctionnement de ces SIG et de leur disponibilité est donc d'une importance capitale. Sans cela les travaux entrepris en matière de normalisation seront sans effet. La France compte sur son territoire environ 130 plateformes d'information géographiques[539] qui participent à diffuser à tous les échelons (territorial, régional et nationale) des informations géographiques à l'ensemble des citoyens. Pour une administration locale, le service d'information géospatiale est un système informatique important en matière de diffusion d'informations pour ses résidents. Étant donné que toutes les informations géographiques gouvernementales sont des biens publics, elles ne doivent pas seulement être utilisées, mais également protégées. Cependant, il n'existe pas de norme ni de ligne directrice officielles concernant la protection contre les risques cyber des services d'information géospatiaux en France. Les grandes lignes de la ligne d'analyse développé par Makoto Hanashima est ici reprise car elle il existe une très forte proximité entre le cas français et japonais comme il sera démontré plus avant dans ce chapitre.

Hanashima souligne que le principal objectif des SIG pour les gouvernements locaux est la gestion des informations géospatiales dans le cadre de l'administration et comme outil d'aide à la décision. De plus, l'utilisation des SIG pour la diffusion d'informations et l'amélioration de l'offre des services publics n'a cessé de se développer ces dernières années. La mise en place de SIG régionaux et locaux contribuant directement à l'amélioration des conditions de vie des habitants, en aidant au développement des politiques d'aménagement, il s'agit comme le souligne également Hanashima *« d'une utilisation souhaitable des ressources publiques »*[540] qui se doit d'être pérenne et protégée. En

---

[537] Hanashima Makoto, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », IASSIST Quarterly, vol. 29, n°4, hiver 2005, pp. 16 – 26.

[538] Noucher Matthieu, « Infrastructures de données géographiques et flux d'information environnementale », NETCOM, 27 janvier 2013. https://journals.openedition.org/netcom/1

[539] Afigéo, « Les plateformes territoriales de données géographiques, état des lieux, enjeux et perspectives », p. 9, juin 2023.

[540] Hanashima Makoto, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », IASSIST Quarterly, vol. 29, n°4, hiver 2005, pp. 16 – 26, p.16.

France, le développement de normes internationales en matière de service cartographique en ligne (WMS) telles que celles de l'OGC, ont permis la diffusion à grande échelle de services d'informations géographiques en ligne à tous les échelons territoriaux. Non seulement cela, mais la diffusion des normes WMS rend possible la mise en réseaux de services en combinant deux ou plusieurs services d'information géographiques entrent eux. L'interconnexion de plusieurs SIG ouvre de nombreuses possibilités, améliore le confort d'utilisation et la diversité des services offerts, mais elle augmente aussi la surface d'attaque en ce qui a trait au risque cyber. Le service fourni par une administration locale ne doit pas menacer la sécurité des habitants. Afin d'empêcher l'utilisation illégale d'informations géographiques appartenant au domaine public, il est indispensable de mettre en place des contre-mesures appropriées en matière de sécurité de l'information. Cependant, au Japon comme en France[541], la mise en place de ces contre-mesures est de la responsabilité de chaque région, département, métropole ou communauté de commune qui met en place et exploite ces systèmes d'information.

De plus, les raisons qui font des données géographiques des données particulièrement importantes à protéger ne sont pas nécessairement évidentes, pas plus que les conséquences d'une corruption ou d'une perte de ces données, il est donc nécessaire ici de les rappeler. Tout d'abord, comme le rappel Hanashima, les informations géographiques produites et gérées par le gouvernement sont des biens publics « dont chacun doit pouvoir profiter commodément ». Par conséquent, elles ne peuvent pas être utilisées uniquement au sein des institutions, mais être *« activement mises à la disposition de la population »*[542], et maintenus autant que possible disponibles. Les informations géographiques possèdent une particularité : elles doivent non seulement être mises à la disposition des citoyens, mais aussi être accompagnées d'outils favorisant leur réutilisation, ce qui permet d'en tirer le meilleur profit. Ainsi, les collectivités locales se doivent de respecter certains critères concernant les données géographiques dont elles ont la charge.

1.1 Les responsabilités des diffuseurs de données géographiques

Tout d'abord, comme l'écrit Hanashima, les diffuseurs de données ont des responsabilités qui peuvent se décliner en sept exigences principales[543] : la charge de garantir la protection de l'information géographique en ce qui concerne la vie privée des citoyens. Ils se doivent également de garantir la

[541] Hanashima Makoto, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », IASSIST Quarterly, vol. 29, n°4, hiver 2005, pp. 16 – 26.
[542] Ibid, p. 20
[543] Ibid, p.20

confidentialité des informations géographiques non divulguées au public qu'ils peuvent être amenés à héberger, ainsi que l'intégrité et l'authenticité des informations géographiques. Ils ont également la charge de la gestion des privilèges d'accès à ces données, ainsi que la prévention de la violation des éventuels droits d'auteur des informations géographiques. Il est donc essentiel pour la puissance publique de s'assurer du maintien de la responsabilité des collectivités locales en matière d'informations géospatiales, et que ces dernières soient attentives aux risques qui pèsent sur leurs infrastructures de données géographiques. Il faut également s'assurer que ces dernières peuvent maintenir la disponibilité du service d'information géographique pour les citoyens [544].

Ainsi, Hanashima souligne que l'altération et la falsification des données sont des problématiques de premier plan pour tout système d'information en ligne. En effet, il peut être très difficile de distinguer les données géographiques falsifiées[545]. Par exemple, lorsque le polygone d'une partition foncière est modifié ou qu'une parcelle inexistante est créée, les premières personnes qui voient la carte sont souvent incapables de détecter la falsification des données géographiques. Certaines données géographiques publiées sur le portail d'une administration locale peuvent être utilisées comme document officiel. Par conséquent, l'utilisateur lambda ne questionnera pas l'authenticité de la carte. Ainsi, la diffusion d'une carte falsifiée par une plateforme SIG locale peut avoir de graves conséquences. Pour contrer ces menaces, l'adoption de normes internationales est essentielle. La norme ISO 19115[546], par exemple, définit le schéma requis pour décrire des informations géographiques et des services au moyen de métadonnées, assurant ainsi une documentation cohérente et facilitant la détection d'altérations. De plus, des initiatives telles que le projet PIGMA[547] en Nouvelle-Aquitaine promeuvent la mutualisation de l'information territoriale en respectant les normes ISO 19115, 19119[548] et 19139[549], renforçant ainsi la fiabilité et l'interopérabilité des données géographiques.

La copie et la distribution illégales de données peuvent également constituer un risque important pour les plateformes de données géographiques. En effet, comme démontré par l'étude d'Hanashima, bien que les informations géospatiales soient des biens publics, toutes ne peuvent pas être reproduites sans condition. Le droit d'auteur est généré même si les informations géospatiales ont

---

[544] https://geomatique-aln.fr/les-defis-de-la-securite-des-donnees-en-geomatique/

[545] Hanashima Makoto, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », IASSIST Quarterly, vol. 29, n°4, hiver 2005, pp. 16 – 26., p. 20 – 21.

[546] ISO 19115-1 : 2014. Information géographique — Métadonnées. Partie 1 : Principes de base, Ed 1, 2014. Source : ISO. https://www.iso.org/fr/standard/53798.html

[547] PIGMA (Plateforme d'échange de données en Nouvelle Aquitaine) est la plateforme d'information de la région Nouvelle Aquitaine. https://portail.pigma.org/pigma/

[548] ISO 19119:2016, Information géographique — Services, Ed. 2, 2016. Source : ISO. https://www.iso.org/fr/standard/59221.html

[549] ISO/TS 19139-1 : 2019, Information géographique — Implémentation de schémas XML, Partie 1 : Règles de codage, Ed 1, 2019. Source : ISO. https://www.iso.org/fr/standard/67253.html

été produites par des institutions publiques[550]. Par exemple, une carte de base peut être protégée en tant qu'œuvre collective, tandis que les représentations symboliques ajoutées, comme des pictogrammes spécifiques, peuvent également être protégées si elles présentent une originalité suffisante. Ainsi, l'utilisation ou la reproduction de ces éléments nécessite l'autorisation des titulaires de droits concernés [551]. Dès lors que la puissance publique fixe les conditions d'utilisation de ces données, toute reproduction qui s'en affranchit constitue une copie illégale[552]. De plus, les bases de données géographiques bénéficient d'une protection juridique spécifique. Le producteur d'une telle base dispose de droits exclusifs sur l'extraction et la réutilisation de la totalité ou d'une partie substantielle de son contenu. Toute reproduction ou distribution non autorisée de ces données constitue une violation des droits du producteur [553]. Hanashima observe également que, lorsqu'une image cartographique est le résultat de l'édition d'un ensemble de données géospatiales, le droit d'auteur existe pour toutes les données. Par conséquent, pour une telle reproduction d'une image cartographique, il est nécessaire d'obtenir l'accord de tous les détenteurs de droits d'auteur. Si une grande quantité de copies illégales ne respectant pas les conditions d'utilisation est distribuée, il existe un risque de violation des droits d'auteur[554]. Une gestion rigoureuse des droits et une attention particulière aux licences d'utilisation sont indispensables pour éviter de telles situations [555].

De la même manière, la falsification ou la suppression des journaux d'audit constitue aussi une menace sérieuse pour la sécurité des systèmes d'information, notamment au sein des administrations locales. Ces journaux sont essentiels pour assurer la traçabilité des actions, détecter les anomalies et garantir la responsabilité des acteurs impliqués[556]. Les informations d'audit, telles que les fichiers journaux d'audit, sont indispensables, car l'obligation de rendre compte est une exigence importante pour une administration territoriale [557]. En outre, la perte de l'obligation de rendre compte d'une administration locale entraîne le risque de voir sa responsabilité juridique engagée. Les journaux d'audit enregistrent les activités sur les systèmes informatiques, fournissant une trace des opérations effectuées. Ils sont cruciaux pour identifier les comportements suspects, enquêter sur les incidents de

---

550 Hanashima, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », op. Cit, p.23

551 Frochot Didier, « Les systèmes d'information géographique et le droit », Archimag, n° 326, pp. 40-41, 1er juillet 2024.

552 Hanashima, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », op. Cit, p.23

553 Grelot Jean-Philippe, « Protection juridique des bases de données géographiques : le point de vue de l'Institut Géographique National », CFC, n° 58, décembre 1998. https://www.lecfc.fr/new/articles/158-article-5.pdf

554 Hanashima, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », op. Cit, p.23

555 Frochot Didier, « Le droit des systèmes d'information géographique », les Infostratèges, 29 septembre 2011.

556 Hanashima, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », op. Cit, p.24

557 Code des relations entre le public et l'administration, Article L300-1, modifié par l'ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration.

sécurité et démontrer la conformité aux réglementations en vigueur. Ainsi, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a dédié un de ses guides aux bonnes pratiques concernant la sauvegarde des journaux d'audit et souligne l'importance de ces derniers pour la protection de tout système d'information en ligne [558]. En effet, la manipulation ou l'effacement des journaux d'audit peut masquer des activités malveillantes, entravant ainsi les efforts de détection et de réponse aux incidents. Une telle altération compromet l'intégrité des systèmes de sécurité et peut entraîner une perte de responsabilité, exposant l'organisation à des risques juridiques. Pour protéger l'intégrité des journaux d'audit, il est recommandé de mettre en place des stratégies d'audit avancées, de définir des politiques d'audit sur les postes de travail et d'identifier les événements critiques à surveiller[559]. Ainsi, la protection des journaux d'audit est essentielle pour maintenir la sécurité des systèmes d'information et assurer la responsabilité des actions au sein des administrations locales. L'adoption de bonnes pratiques en matière de gestion des journaux d'audit contribue à prévenir les altérations et à garantir la conformité aux obligations légales.

Bien que les informations géographiques ne soient pas toutes confidentielles par nature, certains types de données spatiales peuvent révéler des informations sensibles lorsqu'elles sont croisées avec d'autres sources de données, comme le signal également Hanashima[560]. Ce phénomène, désigné dans la littérature anglo-saxonne sous le terme d'inferential disclosure[561], constitue l'un des risques majeurs identifiés par les spécialistes de la *geoprivacy*[562]. Il désigne la possibilité, pour un tiers, de déduire des informations qu'un individu n'a jamais consenti à divulguer, en appariant des données géolocalisées avec des bases de données publiques ou accessibles, registres électoraux, cadastre, annuaires, réseaux sociaux, etc.

Ce risque d'inférence par croisement de données (data linkage risk) est particulièrement prégnant dans le domaine des systèmes d'information géographique, où la précision croissante des localisations facilite les opérations de géocodage inverse (reverse geocoding)[563]. Ainsi, la publication de

---

[558] ANSSI, « Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory », ANSSI-PB-090, 28 janvier 2022. https://cyber.gouv.fr/sites/default/files/2022/01/anssi-guide-recommandations_securite_journalisation_systemes_microsoft_windows_environnement_active_directory.pdf

[559] IBM, « Server audit log settings », IBM Security Directory Server, 21 février 2024. https://www.ibm.com/docs/en/sdse/6.4.0?topic=logging-server-audit-log-settings

[560] Hanashima, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », op. Cit, p.23

[561] L'inferential disclosure désigne la possibilité de déduire des informations sensibles sur un individu à partir de données apparemment non identifiantes. Voir : Drechsler J. et Hu J., « Generating synthetic geocoding information for public release », Journal of Survey Statistics and Methodology, vol. 3, n° 4, 2015, p. 425-445.

[562] Le concept de geoprivacy a été formalisé par Kwan M.-P., Casas I. et Schmitz B. C., « Protection of geoprivacy and accuracy of spatial information: How effective are geographical masks? », Cartographica, vol. 39, n° 2, 2004, p. 15-28. Les auteurs définissent la geoprivacy comme « le droit des individus à empêcher la divulgation de la localisation de leur domicile, de leur lieu de travail, de leurs activités quotidiennes ou de leurs déplacements ».

[563] Le géocodage inverse (reverse geocoding) est l'opération consistant à retrouver une adresse postale à partir de coordonnées géographiques. Voir : Brownstein J. S., Cassa C., Kohane I. S. et Mandl K. D., « Reverse geocoding: Concerns about patient confidentiality in the display of geospatial health data », AMIA Annual Symposium

coordonnées géographiques, même anonymisées, peut permettre de retrouver une adresse, puis d'identifier le nom des occupants par consultation de bases de données tierces[564]. De même, des métadonnées décrivant les caractéristiques d'une zone géographique, niveau de revenus, composition démographique, proximité d'équipements sensibles, peuvent, une fois agrégées, révéler des informations sur des individus ou des groupes spécifiques[565].

La difficulté à anticiper et à prévenir ces risques d'inférence tient à leur caractère combinatoire : ce n'est pas une donnée isolée qui compromet la confidentialité, mais la mise en relation de plusieurs jeux de données, chacun pouvant paraître anodin pris séparément[566]. Cette propriété rend les mesures de protection particulièrement complexes à mettre en œuvre, car elle suppose d'anticiper l'ensemble des croisements possibles avec des sources d'information extérieures au système, exercice par définition impossible à mener exhaustivement. En cas d'exposition d'informations confidentielles résultant d'un tel croisement, la responsabilité juridique de l'entité gestionnaire des données peut être engagée, notamment au titre du Règlement général sur la protection des données (RGPD), qui impose aux responsables de traitement une obligation de moyens en matière de prévention des risques de ré-identification[567].

Pour atténuer ces risques, plusieurs techniques de geomasking ont été développées par la communauté scientifique[568]. Ces méthodes consistent à introduire une perturbation contrôlée dans les données géographiques, décalage aléatoire des coordonnées, agrégation spatiale, génération de données synthétiques, afin de réduire la probabilité de ré-identification tout en préservant l'utilité analytique des données[569]. Le choix d'une technique de masquage appropriée dépend du niveau de risque acceptable et de la finalité des données : une étude épidémiologique nécessitant une précision au niveau du quartier

---

Proceedings, 2005, p. 903.

564 Sur les risques de ré-identification par appariement de données géographiques, voir : « Privacy risk in GeoData: A survey », arXiv, 2024. Les auteurs notent que « publishing a location as coordinates means that these can be plotted on a map and then associated with an address. Address details can then be a powerful key for linking the data associated with those coordinates to specific and identifiable information from other sources ».

565 Sur l'inférence d'attributs personnels à partir de données de voisinage, voir : Mendes R. et Vilela J. P., « Geoprivacy in Neighbourhoods and Health Research: A Mini-Review of the Challenges and Best Practices in Epidemiological Studies », International Journal of Environmental Research and Public Health, vol. 19, n° 21, 2022.

566 Ce caractère combinatoire du risque est analysé dans : Powar J. et al., « SoK: Managing risks of linkage attacks on data privacy », Proceedings on Privacy Enhancing Technologies, 2023, p. 43.

567 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD), notamment les articles 25 (protection des données dès la conception) et 32 (sécurité du traitement).

568 Pour une revue systématique des techniques de geomasking, voir : Zhang M. et al., « Geomasking to Safeguard Geoprivacy in Geospatial Health Data », Encyclopedia, vol. 4, n° 4, 2024, p. 103.

569 Les principales techniques de masquage géographique comprennent : le déplacement aléatoire (random perturbation), l'agrégation spatiale (spatial aggregation), le donut masking (déplacement dans une couronne autour du point réel), et la génération de données synthétiques. Voir : Steffen M. et al., « Data protection strategies for geocoded data: A systematic review », International Journal of Health Geographics, vol. 22, 2023.

n'appellera pas les mêmes mesures qu'une analyse à l'échelle régionale[570]. Toutefois, comme le soulignent Kounadi et Leitner, les efforts déployés pour sensibiliser la communauté scientifique aux risques de divulgation géographique demeurent insuffisants : leur étude de 41 articles publiés entre 2005 et 2012 a révélé que plus de 68 000 adresses personnelles avaient été divulguées sans protection adéquate[571].

L'usurpation d'identité est une menace de premier plan pour tout service ou systèmes mis à disposition en ligne et les systèmes d'information géographiques ne font pas exception. En ce qui concerne les conditions d'utilisation des informations géographiques, la désignation des détenteurs des droits d'auteur ou de la source est requise dans de nombreux cas. Toutefois, lorsqu'il n'existe aucun moyen d'attester l'authenticité de l'auteur, un tiers malveillant peut se faire passer pour l'auteur, et l'utilisateur ne peut pas le savoir[572]. L'information n'est pas nécessairement authentique du seul fait que l'avis de droit d'auteur est indiqué. Il est donc possible que l'avis de droit d'auteur soit utilisé abusivement pour camoufler les informations falsifiées par un tiers. Les normes comme ISO 19157[573] (Qualité des données géographiques) offrent des lignes directrices pour évaluer l'authenticité et la qualité des données, y compris la traçabilité des sources. Ces normes visent à limiter les risques liés à des informations falsifiées. Pour contrer ces menaces, les recherches les plus récentes se tournent vers des technologies comme la blockchain pour trouver des solutions innovantes en matière d'authentification et de certification des données. En créant des enregistrements immuables et vérifiables, la blockchain permet de garantir l'intégrité et la provenance des informations [574]. À titre d'exemple, des plateformes telles que Dock.io proposent des systèmes de vérification basés sur la blockchain pour confirmer l'authenticité des documents et des identités numériques [575]. Cependant ces systèmes sont loin d'être aisé à implémenter ne constitueront probablement pas la norme en matière de cybersécurité pour des plateformes géographiques régionales avant longtemps, si elles le deviennent. Les gestionnaires de données géographiques doivent également veiller à se protéger contre les attaques

---

570 Sur l'arbitrage entre utilité analytique et protection de la confidentialité, voir : Zandbergen P. A., « Ensuring Confidentiality of Geocoded Health Data: Assessing Geographic Masking Strategies for Individual-Level Data », Advances in Medicine, 2014.

571 Kounadi O. et Leitner M., « Why Does Geoprivacy Matter? The Scientific Publication of Confidential Data Presented on Maps », Journal of Empirical Research on Human Research Ethics, vol. 9, n° 4, 2014, p. 34-45.

572 Hanashima, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », op. Cit, p.23

573 ISO 19157:2013 : Information géographique — Qualité des données, Ed. 1, 2013. https://www.iso.org/fr/standard/32575.html

574 Mendiboure Léo, Aymen Chalouf Mohammed et Krief Francine, « A Scalable Blockchain-based Approach for Authentication and Access Control in Software Defined Vehicular Networks », 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, USA, septembre 2020.

575 Truvera, « Blockchain Verification: What is it and how does it work? », 13 janvier 2025. https://www.dock.io/post/blockchain-verification ?

informatiques qui viseraient à rendre inaccessible la plateforme d'information géographique, rendant ainsi les données inexploitables.

Si l'authentification et la certification des données géographiques sont cruciales pour garantir leur intégrité, elles ne suffisent pas à elles seules à protéger les systèmes d'information géographiques contre toutes les menaces. En effet, au-delà des risques liés à l'usurpation d'identité et à la falsification des données, les plateformes géospatiales doivent également faire face à des attaques ciblant directement leurs services en ligne. Ainsi, si les mécanismes de protection visent à garantir l'authenticité des sources, ils doivent être complétés par des mesures de cybersécurité robustes pour prévenir les détournements et les intrusions malveillantes qui peuvent compromettre non seulement la disponibilité, mais aussi la fiabilité des services géospatiaux.

1.2 Anticiper les risques d'attaques informatiques sur les infrastructures de données géographiques

L'attaque par un service non autorisé constitue ainsi une menace importante. En effet, si les normes d'interopérabilité en matière de services web permettent la mise en réseau de plusieurs services Web, elles rendent également possible le détournement de services Web à l'insu de leurs utilisateurs, comme le remarquait déjà Hanashima[576]. Par exemple, des standards tels que WMS (Web Map Service) et WFS (Web Feature Service) facilitent le partage et l'affichage de données géospatiales sur diverses plateformes. Cette interopérabilité est essentielle pour une collaboration efficace entre différents systèmes et organisations. Cependant, cette ouverture présente des vulnérabilités potentielles. Les cyberattaques, telles que les injections de données malveillantes ou les détournements de services web, peuvent compromettre l'intégrité des données géospatiales[577]. Par exemple, une attaque par déni de service (DDoS) peut rendre un service SIG indisponible, perturbant ainsi les opérations qui en dépendent. De plus, l'interception de données sensibles lors de leur transmission entre services interopérables constitue une menace réelle [578]. De même, un service Web détourné par un cyberattaquant peut se voir injecté des informations géographiques altérées, endommageant du même coup le fonctionnement du service.

Comme le souligne Hanashima, il peut arriver également que l'application web hébergeant la plateforme d'information subisse directement une attaque informatique, comme cela a été le cas lors de l'attaque informatique contre le site internet de la région Normandie en 2022, nous reviendrons sur cette attaque plus loin. En général, un service d'information géospatiale est mis en œuvre sous la forme

[576] Hanashima, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », op. Cit, p.23

[577] Ibid

[578] https://www.info.gouv.fr/risques/cyber-destabilisation

d'une application Web. Bien que diverses mesures puissent être mises en œuvre pour assurer la sécurité informatique d'une application Web, il n'est pas facile de créer une application Web sans vulnérabilité. En particulier dans le cas des autorités locales qui ne disposent pas nécessairement du personnel et des compétences nécessaires au maintien en toute sécurité d'un service web. La pénétration d'un service Web de plateforme géographique peut entraîner l'exécution de codes malveillants, le détournement du système entier, son altération, etc[579]. Pour renforcer la sécurité des applications web, plusieurs bonnes pratiques sont recommandées[580]. Il est essentiel de mettre en place des politiques de mots de passe robustes, de chiffrer les données sensibles, d'implémenter une sécurité basée sur la stricte séparation des rôles des utilisateurs, de faire appel à des fournisseurs de sécurité, d'entreprendre régulièrement un audit des activités, de maintenir les logiciels à jour, d'exiger l'utilisation du protocole HTTPS et d'effectuer des tests d'assurance qualité après chaque mise à jour. Ces mesures contribuent à protéger les applications contre diverses menaces, telles que les injections SQL ou les attaques par déni de service[581]. Il existe cependant des normes strictes en matière de sécurité informatique auxquelles la plupart des acteurs du marché se conforment. Par exemple, Esri, adhère aux normes américaines et internationales, ainsi qu'aux bonnes pratiques du secteur en matière de sécurité informatique et de confidentialité. Cela inclut le respect des directives de l'Open Web Application Security Project (OWASP)[582] et des normes ISO 27001[583]. Ces standards garantissent que les plateformes SIG offrent un niveau de sécurité élevé pour protéger les données géospatiales sensibles.

Des erreurs en matière de paramétrage des privilèges d'accès peuvent également avoir de graves conséquences. En règle générale, les informations géospatiales sont constituées des données de nombreux éléments à surveiller comme le souligne également Hanashima[584]. La gestion des privilèges d'accès est cruciale dans les systèmes d'information géographique, car ces systèmes intègrent des données sensibles et variées. Une mauvaise configuration des droits d'accès peut entraîner des fuites d'informations confidentielles ou des accès non autorisés. Ainsi, il est important que les organismes gestionnaires mettent en place des stratégies de Gestion des Privilèges d'Accès (Privilege Access Management : PAM). Le PAM vise à surveiller et à limiter l'accès en créant un système de comptes privilégiés et non privilégiés, garantissant ainsi que seuls les utilisateurs autorisés peuvent accéder à

---

579 Hanashima, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », op. Cit, p.23

580 Interdata, « Comment renforcer la sécurité des applications web face aux cyberattaques ? », 17 juillet 2024. https://blog.interdata.fr/article-securite-des-applications-web-failles-risques-bonnes-pratiques

581 https://www.jitterbit.com/fr/blog/web-application-security-best-practices

582 Open Web Application Security Project, « Secure Coding Practices Quick Reference Guide », décembre 2022. https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/

583 ISO/IEC 27001:2022 : Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences, Ed.3, 2022. https://www.iso.org/fr/standard/27001

584 Hanashima, « Consideration for Information Security Issues in Geospatial Information Services of Local Governments », op. Cit, p.23

des données spécifiques [585]. Cette gestion peut être relativement complexe à mettre en place, ce qui complique la tâche des petites structures, notamment dans les territoires. Cependant, si la configuration d'un privilège d'accès est mal configurée, cela peut entraîner immédiatement une fuite d'informations confidentielles et poser divers problèmes de sécurité. Les erreurs de configuration des privilèges d'accès peuvent être dues à la complexité croissante des systèmes, au manque de formation du personnel ou à l'absence de politiques de gestion des droits. L'ensemble de ces problèmes sont récurrents dans certains territoires qui ne disposent pas toujours des moyens financiers et humains pour implémenter des mesures efficaces en matière de cybersécurité. Ces erreurs peuvent entraîner des fuites de données sensibles ou des accès non autorisés, compromettant ainsi la sécurité des informations. Il apparaît donc essentiel de mettre en place des politiques de gestion des accès robustes et de former le personnel aux meilleures pratiques en matière de sécurité. Pour renforcer la sécurité des informations, l'adoption de normes internationales, telles que l'ISO/IEC 27001 est recommandée[586]. Cette norme fournit un cadre pour établir, mettre en œuvre, maintenir et améliorer continuellement un système de gestion de la sécurité de l'information. Elle aide les organisations à identifier les risques liés à la sécurité de l'information et à mettre en place des contrôles pour les gérer ou les éliminer. Face à ces menaces, l'adoption de normes internationales reconnues aide à renforcer la résilience des plateformes d'information géographiques en diffusant de bonnes pratiques en matière de qualité des données, notamment.

1.3 Les normes : un outil clé pour développer la résilience des plateformes d'information géographique

Les erreurs dans les données géographiques posent des défis significatifs, notamment en matière de détection et d'interopérabilité. Il est ainsi très difficile de découvrir les erreurs présentes au sein d'informations géographiques. Bien qu'un contrôle géométrique ou encore un contrôle numérique des informations d'attribut par un ordinateur soit possible, il existe de nombreuses erreurs indétectables par ces contrôles. Par exemple, des incohérences logiques ou des erreurs sémantiques peuvent passer inaperçues sans une analyse humaine approfondie [587]. L'influence d'un service fourni par un gouvernement local indépendant s'arrête à cette région, mais, lorsque les données se retrouvent

---

585 Ledesma Josue, « Qu'est-ce que la gestion des accès à privilèges (PAM) ? », Varonis, 6 octobre 2023. https://www.varonis.com/fr/blog/gestion-des-acces-a-privileges ?

586 ISO/IEC 27001:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences, Ed.3, 2022.

587 1Spatial, « Le petit livre de la Gestion des données Géospatiales », 2021. https://1spatial.com/media/roolaoot/006931_1spatial_little-book-data-management_a5_v5_1-4-fr-single-pages.pdf

distribuées à travers plusieurs plateformes, il existe un risque que des données erronées soient diffusées dans de nombreux services. Ainsi, l'interconnexion rendue possible par la diffusion des normes internationales peut également propager des erreurs présentes dans un jeu de données à d'autres systèmes, amplifiant ainsi leur impact. Les normes d'interopérabilité, telles que celles développées par l'OGC, fournissent des modèles uniformes pour créer, reproduire et conserver des données géographiques, mais ces normes ne garantissent pas l'absence d'erreurs dans les données échangées. Cependant, l'adoption de normes internationales, notamment en matière de cybersécurité et de qualité des données, permet de faciliter le contrôle de la qualité des données par les opérateurs qualifiés et contribue à renforcer la résistance des plateformes d'information aux attaques informatiques. Les erreurs dans les données géographiques peuvent entraîner des décisions inappropriées, surtout dans des domaines critiques, tels que la gestion des urgences, l'urbanisme ou l'environnement. À titre d'exemple, une erreur dans la cartographie des zones inondables pourrait conduire à une planification inadéquate des infrastructures, augmentant les risques pour les populations locales [588]. Les utilisateurs supposent souvent que les données sont de bonne qualité, surtout lorsque celles-ci sont mises à leur disposition par la puissance publique. Cette croyance peut conduire à des surprises désagréables et à des incidents résultant d'usages inappropriés des données.

En conclusion, il est essentiel de mettre en place des processus rigoureux de contrôle de la qualité des données géospatiales et de sensibiliser les utilisateurs aux limites potentielles de ces données. L'adoption de normes d'interopérabilité, telles que la norme ISO 19157 et la formation continue des professionnels peuvent aider à atténuer les risques associés aux erreurs dans les données géospatiales.

Les systèmes d'information géographiques dépendent fortement de l'interopérabilité entre divers services web pour fonctionner efficacement. Cette dépendance comporte des risques significatifs, notamment en cas de défaillance d'un service essentiel, ce qui peut perturber l'ensemble du système. Les normes jouent un rôle crucial pour atténuer ces risques en établissant des protocoles communs qui facilitent la communication et la résilience entre les systèmes [589]. Lorsque le service d'information géospatiale fonctionne sur la base de l'interopérabilité des services Web, la défaillance d'un service affecte immédiatement les autres services. Par exemple, si le service qui fournit le fond de carte s'arrête, les autres services ne peuvent pas continuer à fonctionner. Cette situation est exacerbée

---

[588] Bédard Yvan et Gervais Marc, « Gestion des risques liés à la qualité des données géospatiales », Université Laval, Centre de recherche en géomatique, 28 décembre 2009. https://fr.slideshare.net/slideshow/gestion-des-risques-lis-la-qualit-des-donnes-gospatiales/2785437.; Troispoux Gilles, « La qualité des données géographiques, État des lieux pour un débat », Certu, 29 octobre 2010. https://www.crige-paca.org/wp-content/uploads/2021/11/Reflexion_sur_la_qualite_des_donnees_geographique.pdf

[589] Lambois Marie et Drouadaine Clément, « Les services Web de l'OGC : Principe et standards », 1er octobre 2018. https://eden.ign.fr/wp-content/uploads/ISN-18.097-Webservices-partie-1.pdf

par la concentration du marché autour de quelques fournisseurs majeurs, comme Esri, créant des points de défaillance uniques pouvant affecter des millions d'utilisateurs. Par conséquent, une telle défaillance de l'interopérabilité entre les systèmes constitue une menace sérieuse pour tout service d'information géographique. Il existe plusieurs mesures pour atténuer ce risque. Assurer une redondance des services peut être une première mesure. La redondance des services consiste à dupliquer des composants ou des systèmes critiques afin d'assurer une continuité de service en cas de défaillance. Dans le contexte des SIG, cela peut impliquer la duplication de serveurs, de bases de données ou de services cartographiques. Par exemple, l'utilisation de services de stockage sur le cloud offre différents niveaux de redondance pour sécuriser les données, garantissant ainsi leur disponibilité même en cas de panne matérielle ou logicielle [590]. La surveillance proactive consiste dans le suivi en temps réel des performances et de l'état des systèmes pour détecter et anticiper les problèmes avant qu'ils n'affectent les opérations. Dans le cas des plateformes d'information géographique, cela peut inclure la supervision de l'état des infrastructures et la planification de la maintenance préventive, afin de réduire les risques de défaillance. Enfin, l'utilisation de caches locaux pour les données critiques permet de stocker localement des copies des données essentielles pour en garantir l'accès même en cas d'interruption du service principal [591]. Ces stratégies contribuent à renforcer la résilience des infrastructures géospatiales face aux défaillances potentielles. En France, le Référentiel Général d'Interopérabilité (RGI)[592] fournit un cadre de recommandations pour assurer l'interopérabilité des systèmes d'information de l'administration. Ces normes et recommandations permettent aux différents systèmes de communiquer efficacement, réduisant ainsi la dépendance à un fournisseur unique et améliorant la résilience globale.

Ainsi, comme nous l'avons vu, de nombreuses menaces pèsent sur les infrastructures de données géographiques et peuvent mettre en danger la bonne disponibilité de ces données pour les citoyens. La falsification des données constitue de loin la menace la plus importante. En effet, les falsifications de données géographiques sont souvent difficiles à identifier pour les non-initiés et pourraient mettre en danger la bonne réalisation de certains projets d'aménagement du territoire, ou a minima retarder leur exécution si des erreurs dans les données sont détectées a posteriori. Au cœur de ces préoccupations, les problèmes générés par un manque d'interopérabilité entre les différentes composantes d'un système d'information en ligne constituent une menace d'importance. Une simple

---

590 FasterCapital, « Comprendre La Redondance Des Données », 2 juin 2024. https://fastercapital.com/fr/sujet/comprendre-la-redondance-des-donn%C3%A9es.html

591 AWS, « Pilier Efficacité des performances », AWS Framework Well-Architected, p. 65, 2024. https://docs.aws.amazon.com/fr_fr/wellarchitected/latest/performance-efficiency-pillar/wellarchitected-performance-efficiency-pillar.pdf

592 Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État, « Référentiel Général d'Interopérabilité : Standardiser, s'aligner et se focaliser pour échanger efficacement », version 2.0, décembre 2015. https://www.numerique.gouv.fr/publications/interoperabilite/

défaillance dans l'interopérabilité d'un composant d'un système d'information peut entraîner l'arrêt total de ce dernier. Les standards ont donc un rôle à jouer de plus en plus important, et se doivent d'incorporer autant que faire ce peu des mesures en matière de cybersécurité. Les standards en matière d'information géographique sur lesquelles s'appuient les infrastructures d'information géographique régionales et nationales sont aujourd'hui conçus par le Conseil national de l'information géolocalisée (CNIG). La place du CNIG dans l'écosystème normatif national concernant les données géographiques nécessite d'être étudié en détail, en ce qu'il pourrait constituer le principal canal dans l'incorporation de normes de cybersécurité dans les normes nationales en matière de données géographiques.

2. Le CNIG, un acteur essentiel de la normalisation nationale

Le Conseil national de l'information géographique, devenu en 2022 le Conseil national de l'information géolocalisée (CNIG), est bien plus qu'un simple organe technique de standardisation. Il constitue « l'instance de dialogue entre tous les acteurs de l'information géographique, producteurs comme réutilisateurs », un forum où se négocient les règles communes de production et d'usage des géodonnées, adapté aux évolutions du numérique[593]. À l'heure où le cyberespace et les données numériques s'imposent comme de nouveaux terrains de rivalités, la gouvernance des normes géographiques prend une dimension stratégique. En effet, l'émergence d'un cyberespace structuré par des rapports de force géopolitiques croissants » fait des standards géospatiaux un enjeu de souveraineté et de pouvoir. Dès lors, comprendre le rôle du CNIG exige de l'inscrire dans les jeux de pouvoir multiéchelles : au niveau national, où État, collectivités, agences publiques et acteurs privés s'affrontent ou coopèrent pour orienter la normalisation, et au niveau international, où s'entrecroisent les influences de l'Union européenne, comme la directive INSPIRE, des organismes de standardisation (OGC, ISO), de grandes puissances, et des réseaux d'agences, tels que EuroGeographics en Europe.

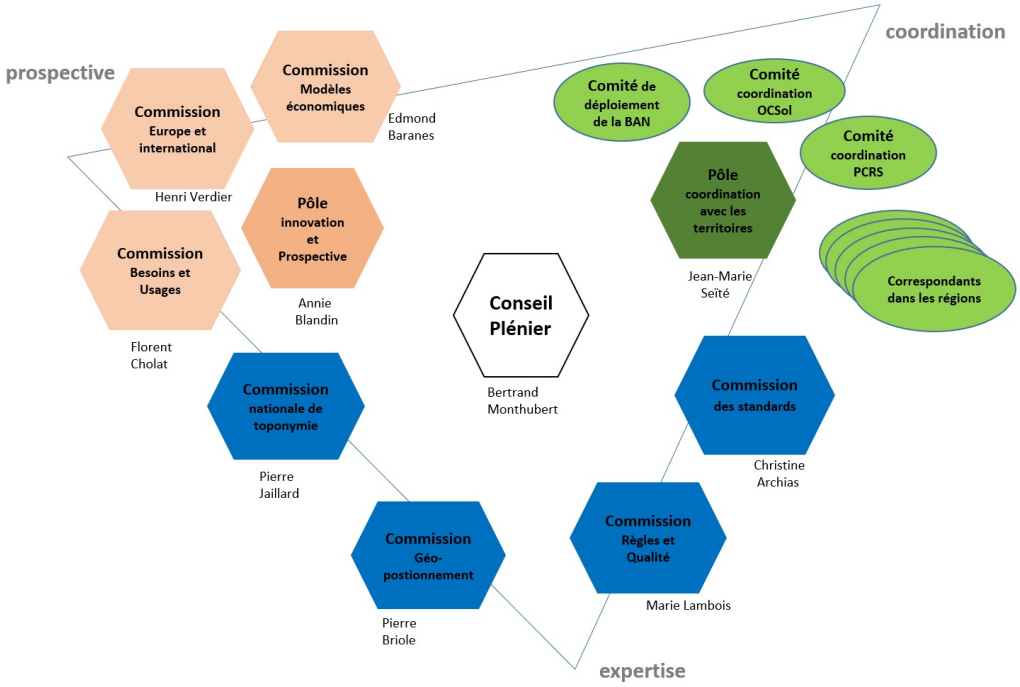
Le CNIG s'organise en divers pôles et commissions en charge de coordonner les différents travaux de normalisation (Figure 15).

- Le pôle « Coordination avec les territoires » est chargé d'organiser la coordination entre les acteurs nationaux et territoriaux.
- Le pôle "Innovation et prospective" est chargé de traiter des sujets prospectifs et d'innovation et d'identifier les sujets qui orienteront les travaux du CNIG.
- La commission des « Standards » est chargée d'assurer la coordination et la concertation des acteurs permettant la mise en œuvre de standards nationaux de données géographiques cohérents avec les directives européennes.
- La commission « Règles & Qualité », est chargée d'assurer la coordination et la concertation des acteurs sur les règles d'utilisation, de qualité, des données et métadonnées cohérentes avec les directives européennes.
- La commission « GeoPositionnement », est chargée de l'approfondissement, de la mutualisation et de la diffusion des connaissances dans les « techniques de géopositionnement à terre, en mer, sous la terre, sous les mers, dans les airs ou dans l'espace ».

[593] Marzolf Emile, « La gouvernance de la donnée géographique mute pour s'adapter au numérique », acteurspublics, 8 septembre 2022. https://acteurspublics.fr/articles/la-gouvernance-de-la-donnee-geographique-mute-pour-sadapter-au-numerique/. Consulté le 22 mars 2024.

- La commission nationale de toponymie est chargée de contribuer à la conservation et au développement cohérent du patrimoine toponymique de la France.
- La commission « Europe et International » est chargée d'assurer la concertation entre les acteurs en vue de renforcer l'adaptation à la mondialisation et la présence française sur les marchés européens et internationaux.
- La Commission « Besoins et Usages » est chargée d'identifier les arrivées, nécessités et demandes de nouvelles productions d'information géographique ou géolocalisée.
- La commission Modèles économique est chargée de se saisir des thématiques de modèles économiques de production, de diffusion, d'utilisation des données géolocalisées et de connaissance économique d'écosystème des géodonnées.

Figure 15 : Organisation du CNIG



Source : *Site officiel du CNIG (2023)*

Les commissions et pôles du CNIG sont en charge d'élaborer les normes nationales en créant des groupes de travail, similaires à ceux des organisations internationales de normalisation. Ces groupes de travail rassemblent les acteurs prêts à s'impliquer activement dans la conception des normes. Ces groupes n'excèdent généralement pas une dizaine de personnes. Cela tient autant au fait que trouver des acteurs prêts à s'investir activement dans la production normative n'est pas toujours

aisé, mais également, car, même en cas de forte affluence d'acteurs prêts à s'impliquer, dépasser un tel nombre de participants risquerait de rendre les réunions du groupe de travail difficile à organiser. Le CNIG est également en charge de produire des guides afin d'aider les collectivités territoriales dans la production de données géographique sur leur territoire. Ces guides précèdent parfois la création d'une norme sur le même sujet. L'ensemble des normes produites par le CNIG sont référencées sur le site data.gouv.fr [594]. Les normes développées par le CNIG couvrent un ensemble très large de thématiques, visant à répondre aux besoins nationaux en matière de production de données géolocalisées. On retrouve ainsi des thématiques, telles que l'aménagement, les risques, les forêts, l'urbanisme, l'occupation des sols, la biodiversité, l'urbanisme ou encore les réseaux électriques. La liste des normes publiées par le CNIG au 1er mars 2026 s'organise comme suit (Figure 16)

[594] https://schema.data.gouv.fr/schemas.html?q=&label=CNIG

Figure 16 : Liste des normes validées par le CNIG au 1er mars 2026

Thématique	Nom du standard	Version	Date	Lien
Adresse	Standard Adresse	V1	oct-2024	lien
Aménagement	Sites Économiques	v2023-10	oct-2023	lien
Aménagement	Friches	v2023-12	déc-2023	lien
Aménagement	Opérations d'aménagement	v2025-03	mars-2025	lien
Mobilité	Accessibilité	V.2021-10 (rev 2025-03)	juin-2023	lien
Réseaux	Plan de corps de rue simplifié (PRCS)	V.2.0	sept-2017	lien
Réseaux	Socle des Réseaux (STAR-DT)	V1.0	mars-2020	lien
Risques	Standard Risques modèle commun	V1	déc-2024	lien
Risques	Standard Risques profil Plan de prévention des risques	V1.0.1	juin 2025	lien
Urbanisme	Documents dématérialisés d'urbanisme	PLU/CC/SCOT/PSMV/SUP	juin-2025	voir page Ressources DDU
Occupation du sol	Occupation du sol à grande échelle (OCSGE)	V1	déc-2014	lien
Biodiversité	Continuité écologiques régionales (CER)	V2018-9	sept-2018	lien
Réseaux	GRACE THD	V3.0.1	dec-2024	lien
Forêts	Dessertes pour le transport de bois	V1	mars-2019	lien
Urbanisme	Éclairage extérieur	V1.1	nov-2022	lien
Réseaux	Réseaux électriques (STAR-Elec)	V1.02	nov-2022	lien
Réseaux	Réseaux enterrés des eaux - (STAR-Eau)	V1.0	déc-2024	lien
Paysages	Paysages	V1.0	juil-2024	lien
divers	Standards Covadis		2008 - 2019	lien

Source : *Site officiel du CNIG (2026)*

En 2026, sept projets de normes sont également en préparation, ils se présentent comme suit (Figure 17) :

Figure 17 : Liste des projets de normes en préparation au sein du CNIG au 1er mars 2026

Thématique	Nom du standard	statut	Date	Lien
Littoral	standard Gimel	GT en cours	2022	lien
Bâtiment	référentiel des bâtiments	GT en cours	nov-2022	lien
Bâtiment	standard ERP	GT en cours	nov-2021	lien
Mobilités	standard Routes/voies	GT en cours	2023	lien
Énergie	standard énergies renouvelables	GT en cours	nov-2022	lien
Aménagement	standard de vues immersives	GT en cours	2022	lien
Biodiversité	standard Espaces naturels protégés	GT en cours	oct-2024	lien

Source : *Site officiel du CNIG (2026)*

Comme au sein des organisations internationales de normalisation, le CNIG suit une procédure stricte durant la création d'un standard afin de garantir un maximum de participation et un respect du principe de consensus qui sous-tend la création de tout standard. Ce processus est composé de cinq étapes. Tout d'abord, le projet de standard doit être présenté devant la commission Besoins et Usages du CNIG et soumis au vote, afin de pouvoir exposer les raisons justifiant de la mise en chantier d'un

projet de standard. Cela permet également d'inviter de nouveaux acteurs potentiellement intéressés à se joindre au projet. Une fois le projet de standard validé, le groupe de travail lance une consultation la plus large possible auprès des potentiels acteurs intéressés par ce projet de norme. Une fois le travail effectif débuté, un appel à commentaire public est lancé afin de recueillir un maximum d'avis. Cette étape cruciale permet de vérifier que le standard qui est en train d'être construit répond bien aux attentes des acteurs du milieu. Les principaux commentaires sont résolus en collaboration avec ceux qui les ont soumis. Cette étape permet de garantir l'aspect consensuel du standard en cours d'écriture. Un grand nombre de commentaires tend à indiquer un vaste engagement des principaux organes intéressés par ce standard et permet généralement, une fois ces derniers résolus, une large adoption du standard. Une fois la rédaction du standard terminé, il est présenté à la commission de standards du CNIG qui valide ou rejette le standard par un vote à main levée. Une fois le standard validé, il peut être utilisé immédiatement par les acteurs concernés. La dernière étape a lieu lors du prochain conseil plénier du CNIG où tous les standards précédemment validés sont examinés une dernière fois et officiellement adoptés. Il est à noter également que l'ensemble des groupes de travail du CNIG sont encadrés par un mandat, disponible en ligne, présentant la raison d'être du standard, le contexte réglementaire et son fonctionnement (notamment les organisations en charge du pilotage et de l'animation du GT comme le Cerema ou l'IGN).

La mise à disposition de l'ensemble des éléments relatifs aux standards, qu'il s'agisse de ceux en cours de production ou de ceux déjà validés, est également une composante essentielle du succès des standards. Cela permet à un maximum de participants potentiels, même s'ils sont en dehors de la communauté d'experts techniques concernés, de se renseigner sur les travaux du CNIG et éventuellement d'y participer. Cette ouverture quant aux procédures normatives est importante pour renforcer l'intérêt et la participation du grand public au processus normatif, processus pour lesquels ils se passionnent rarement, mais où ils peuvent également trouver un intérêt. L'ensemble de la société est concerné par la façon dont les données géographiques sont collectées et diffusées et, par conséquent, les processus normatifs qui sous-tendent leurs productions doivent également faire l'objet d'une certaine attention de la part du grand public. Si aujourd'hui, les personnes qui ne sont ni experts techniques ni métiers restent rares en termes de participation, maintenir une transparence maximale reste un enjeu majeur pour les normes géographiques nationales.

Au-delà du caractère éthique de la transparence dans la production des standards, le travail de concertation permet de faire émerger un maximum de cas d'usage, d'où l'importance de consulter le plus d'experts « métier »[595] possibles. La consultation permet également de dresser l'inventaire des

[595] On entend ici par expert « métier » les personnes en charge d'appliquer le standard une fois validé. Il peut s'agir de personnes travaillant au sein des collectivités locales ou de sociétés privés en charge de collecter et/ou de gérer les

données similaires à celles sur lesquelles porte le standard et qui déjà produite ou en cours de production par certains acteurs. Cela permet à terme de s'inspirer des données déjà produites et de dégager des dénominateurs communs entre ces dernières afin de pouvoir réutiliser au maximum le travail déjà effectué. Enfin, consulter un maximum de parties prenantes permet également de faciliter l'appropriation du standard et sa diffusion. Les consultations dans le cadre des standards CNIG prennent la forme d'appels à contribution en ligne, mais ce n'est pas la seule forme de consultation possible. Ces derniers peuvent également prendre la forme d'entretiens avec des spécialistes, de façon individuelle ou collective, afin de recueillir leurs besoins. Enfin, il peut arriver que les consultations prennent la forme d'ateliers ouverts à tous afin de recueillir les avis de personnes situés en dehors de la communauté d'experts techniques et métiers. Cette forme de consultation est importante afin de faciliter la participation du grand public à la production de standards et de le familiariser avec les enjeux de la normalisation. Ces consultations ouvertes sont de loin les plus dures à mettre en place, du fait à la fois d'un certain désintérêt du grand public pour la normalisation, qui naît principalement d'une méconnaissance du sujet. On peut citer également, comme difficulté, l'autocensure des participants, là encore lié à leur méconnaissance de la normalisation, mais également du domaine technique concerné par la norme étudiée.

Même après la publication d'un nouveau standard et une consultation efficace, il est important de surveiller l'application effective du standard. En effet, même une large consultation ne garantit pas toujours une large adoption du standard proposé. De nombreux obstacles peuvent se dresser même après la publication d'un standard. Certains producteurs de données peuvent être réfractaires à changer leur méthode de production face à l'arrivée d'une nouvelle norme. Ainsi, le suivi d'un standard après sa publication est presque aussi important que sa création elle-même si l'on souhaite voir le standard adopté massivement. Cette étape n'apparaît pas toujours évidente à l'ensemble des acteurs impliqués dans le processus normatif et, si elle est ignorée, peut aboutir à des standards de données devenant de facto inutiles, car non appliqués. Pour remédier à cela, plusieurs méthodes peuvent être employées. Après la publication des résultats de recherche, des réunions de concertation collaborative peuvent être organisées en collaboration avec les organismes responsables de la direction des normes et les organismes et personnes chargées de les appliquer. Publier avec le standard des exemples d'implémentation aide également grandement les utilisateurs finaux du standard. Mettre à disposition de la documentation en ligne, comme des guides d'implémentation, ou des liens vers des outils de validation comme celui d'Etalab[596] ou Validata[597] permet également de venir en aide aux personnes en

données.

[596] https://publier.etalab.studio/fr

[597] https://validata.fr/

charge d'implémenter le standard. Enfin, des entretiens avec des producteurs de logiciels métiers peuvent également être essentiels afin de faciliter l'intégration du standard de données au sein de ces outils employés par les professionnels du domaine. Ces entretiens peuvent avoir lieu durant la production du standard, mais également après sa publication, et ce, en collaboration avec les clients de ces entreprises, qui sont souvent les collectivités locales. En effet, il est difficile de contraindre de telles sociétés autrement qu'en passant par leurs clients. Si ces derniers démontrent d'une volonté forte d'adopter le standard, les sociétés productrices de logicielles métiers se voient alors forcées d'adapter leurs outils pour rendre la production des données respectant ces standards plus aisés. Produire un standard est donc un travail de longue haleine, qui doit s'envisager dans la durée, depuis sa conception jusqu'à son exploitation.

On le voit, les standards développés par le CNIG couvrent un très large éventail de besoins et offrent les conditions essentielles à l'exploitation en bonne et due forme de ces données. Le développement de ces standards fait appel à un large ensemble d'acteurs nationaux, en particulier à l'échelle régionale, où l'on retrouve au premier plan les gestionnaires de plateformes d'information géographiques. Ces plateformes s'appuient sur les standards CNIG, non seulement pour diffuser les informations collectées aux citoyens, mais offrent également, par le biais de leurs services en ligne, un grand nombre d'outils à leurs utilisateurs, permettant de faire fructifier les données et d'en tirer une plus grande valeur ajoutée. Cependant, l'ensemble de ces plateformes présentent des visages très hétérogènes en termes de mode de gouvernance, de financement ou encore de moyens humains.

2.1 Naissance, transformations et enjeux de pouvoir institutionnels du CNIG

Fondé le 26 juillet 1985, le Conseil national de l'information géographique (CNIG), est en charge de la coordination des acteurs de la production de données géoréférencées sur le territoire français. Le CNIG est placé sous la direction du ministre chargé du développement durable. Le CNIG a été fermé le 31 décembre 2008, à la suite de la création d'une commission interministérielle (la COVADIS) en charge de produire des géostandards pour répondre aux exigences de la directive européenne INSPIRE publiée en 2007. La COVADIS était placée directement sous la direction du ministère de l'Écologie, du Logement et de l'Agriculture, la COVADIS était en charge de produire des normes pour l'ensemble des données géographiques utilisées par ces ministères. Le CNIG a été de nouveau ouvert le 25 septembre 2013, à la suite de la publication du décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géolocalisée [598], abrogeant le précédent décret fondateur du 26 juillet 1985[599]. Dans son champ de compétence, le CNIG a pour but, entre autres *« De formuler et de rendre publics des avis, propositions, recommandations, guides ou standards relatifs aux enjeux, à la production, à la qualification et à la diffusion de l'information géolocalisée »*[600]. De ce fait, le CNIG est aujourd'hui la principale instance gouvernementale en charge de la production de normes nationales concernant les informations géolocalisées. À la suite de la publication de la directive INSPIRE, le CNIG a été désigné comme l'organe de coordination national français, comme prévu aux articles 18 et 19.2 de la directive [601].

Le CNIG joue aujourd'hui un rôle central dans la production de données géoréférencées en France, et notamment concernant la création et la diffusion de normes en la matière. Dès sa création l'ambition du CNIG est de *« mettre tous les acteurs autour de la table pour s'entendre sur des règles partagées »*[602]. Il s'agit alors d'un contrepoids institutionnel face à l'IGN, opérateur historique de la cartographie nationale. En effet, le CNIG doit être à l'origine un moyen d'ouvrir la gouvernance des normes au-delà du seul champ de l'agence nationale de cartographie. Ce besoin d'une instance collégiale reflète ainsi une rivalité feutrée entre l'IGN, bras armé technique de l'État, et une myriade

---

598 Décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géolocalisée

599 Décret n° 85-790 du 26 juillet 1985 relatif au rôle et à la composition du conseil national de l'information géographique.

600 Décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géolocalisée, article 1.

601 Directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE), article 18 et 19.2.

602 Marzolf Emile, « La gouvernance de la donnée géographique mute pour s'adapter au numérique », acteurspublics, 8 septembre 2022. https://acteurspublics.fr/articles/la-gouvernance-de-la-donnee-geographique-mute-pour-sadapter-au-numerique/. Consulté le 22 mars 2024.

d'autres acteurs (ministères, collectivités locales, organismes publics ou privés) désireux de participer à la définition des standards. L'histoire du CNIG est ainsi marquée par des soubresauts institutionnels significatifs, symptomatiques de ces luttes d'influence.

Fin 2008, le CNIG est brutalement supprimé à la suite de la création en parallèle d'une commission interministérielle nommée COVADIS, chargée de produire des géostandards conformes aux exigences de la directive européenne INSPIRE. Cette mise en sommeil du CNIG traduisait la volonté de certains ministères, notamment le ministère de l'Écologie, de recentrer la normalisation géographique dans un cadre plus étroitement contrôlé par l'État. La COVADIS, placée sous l'autorité directe du ministère de l'Écologie, du Logement et de l'Agriculture, visait à élaborer des normes pour les données utilisées par ces ministères. On assiste là à un rapport de force institutionnel, puisque la coordination ouverte et multiacteur du CNIG a été un temps éclipsée par une structure technocratique restreinte, soulignant le souhait de l'État de prendre la main sur l'alignement de la France aux normes européennes. Cependant, en 2011, un décret a recréé le CNIG, opérationnel à nouveau à partir de 2013, en lui conférant explicitement le rôle d'organe national de coordination prévu par INSPIRE. Autrement dit, l'Union européenne a en quelque sorte contraint la France à restaurer une arène de concertation nationale sur les standards géographiques. Depuis 2013, le CNIG a été réinstallé auprès du ministre chargé du Développement durable, avec pour mission officielle *« D'informer et de conseiller le Gouvernement »*[603] sur l'information géolocalisée et de formuler recommandations, avis, guides et standards en ce domaine. Il redevient alors la principale instance gouvernementale en charge de la production de normes nationales pour les informations géographiques. Le fait qu'INSPIRE exige une structure de coordination nationale (articles 18 et 19 de la directive)[604] a renforcé la légitimité du CNIG, désormais formellement désigné comme point de contact INSPIRE en France. Cet épisode souligne également comment une norme supranationale, ici européenne, peut rebattre les cartes au niveau national. Ainsi, la France a dû adapter sa gouvernance des données en rouvrant un espace de dialogue plus large. Le cadre européen a donc permis de redonner du pouvoir aux acteurs non étatiques pour participer à la normalisation.

---

603 Décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géolocalisée

604 Directive 2007/2/CE du Parlement Européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE), article 18 (18) : *« Dans certains cas, les séries et services de données géographiques liés aux politiques communautaires ayant une incidence directe ou indirecte sur l'environnement sont détenus et exploités par des tiers. Les États membres devraient donc offrir aux tiers la possibilité de contribuer aux infrastructures nationales, pour autant que la cohésion et la facilité d'utilisation des données géographiques et de services correspondants offerts par ces infrastructures n'en soient pas affectées. »* ; article 19 (19) : *« L'expérience, dans les États membres, a démontré qu'il était important, pour la réussite de la mise en place d'une infrastructure d'information géographique, qu'un nombre minimal de services soit mis gratuitement à la disposition du public. Il convient donc que les États membres proposent gratuitement, au minimum, des services de recherche et, moyennant le respect de certaines conditions, de consultation des séries de données géographiques »*. Disponible ici : Directive - 2007/2 - EN – EUR-Lex. Consulté le 12 septembre 2025.

À partir des années 2020, le CNIG connaît une nouvelle évolution stratégique. Sous l'impulsion du rapport parlementaire de Valéria Faure-Muntian (2018) sur *Les données géographiques souveraines*, sa mission est élargie et sa composition enrichie afin d'être plus « *volontariste* »[605]. Le décret du 30 août 2022 consacre ce changement en substituant *« information géolocalisée »* à *« information géographique »* dans son intitulé[606]. Si ce glissement sémantique peut paraître anodin en apparence, il marque en réalité un tournant important dans l'extension du champ d'action du CNIG. Ce dernier ne s'occupe plus seulement de la cartographie classique, mais de toute donnée comportant une composante spatiale, qu'il s'agisse d'une simple adresse, d'un capteur urbanistique ou de big data territoriaux. Cette refondation, confiée à Bertrand Monthubert, nommé président du CNIG en 2021[607] et soutenue par la ministre de la Transition écologique de l'époque, vise à relancer au plus vite l'action du CNIG dans la coordination des géodonnées et à conforter son rôle pivot de pilotage. Ce changement a permis de redonner au CNIG un leadership affirmé dans la gouvernance des données géolocalisées, à l'heure où se multiplient des producteurs de données extérieurs à l'État. La composition du conseil plénier est ainsi passée de 34 à 43 membres, intégrant dorénavant des acteurs jusqu'alors absents, tels que les ministères des Transports et des Affaires étrangères, témoignant ainsi de l'intersectorialité du sujet, Administrateur général des données (Dinum), INSEE, Office français de la biodiversité, mais aussi des associations comme OpenData France et OpenStreetMap France[608]. L'entrée de ces derniers est symboliquement forte. En effet, l'une représente les collectivités locales engagées dans l'ouverture des données, l'autre la communauté du libre qui produit le principal concurrent ouvert à Google Maps. Ce faisant, le CNIG s'affirme comme lieu de convergence d'intérêts variés, incluant désormais les partisans des communs numériques aux côtés des grands corps de l'État. Cet élargissement répond donc à la critique formulée dans le rapport de la députée Faure-Muntian, d'une composition trop étroite et *« insuffisamment volontariste »*[609], soulevée par certains qui reprochaient au CNIG de ne pas avoir pleinement joué son rôle faute de moyens propres et d'une tutelle trop indifférente. Cependant, des tensions subsistent quant à son positionnement institutionnel et toutes les recommandations du rapport Faure-Muntian n'ont pas été suivies d'effet. Ainsi, le rapport préconisait, par exemple, de placer le CNIG auprès du Premier ministre, avec un secrétariat assuré par la direction du numérique de l'État

---

605 Faure-Muntian Valéria, *« Les données géographiques souveraines »*, Rapport au gouvernement, juillet 2018, p. 31. Rapport_DonneesGeographiquesSouveraines.pdf. Consulté le 12 septembre 2025.

606 Décret n° 2022-1204 du 30 août 2022 modifiant le décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géographique, article 1. Décret n° 2022-1204 du 30 août 2022 modifiant le décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géographique – Légifrance. Consulté le 12 août 2025.

607 Arrêté du 9 avril 2021 portant nomination au Conseil national de l'information géographique. Arrêté du 9 avril 2021 portant nomination au Conseil national de l'information géographique – Légifrance. Consulté le 12 août 2025.

608 La liste des membres du conseil plénier du CNIG est disponible sur le site du CNIG. Membres du CNIG | Conseil national de l'information géolocalisée. Consulté le 13 aout 2025.

609 Faure-Muntian Valéria, *« Les données géographiques souveraines »*, Rapport au gouvernement, juillet 2018, p. 31. Rapport_DonneesGeographiquesSouveraines.pdf. Consulté le 12 septembre 2025.

(DINSIC), afin de lui donner le poids politique interministériel qui lui fait défaut[610]. Actuellement logé au ministère de la Transition écologique, le CNIG souffre en effet d'une portée parfois limitée face aux autres ministères. Le hisser au niveau du Premier ministre renforcerait sa capacité à arbitrer les rivalités entre administrations et à impulser une vision transversale de la normalisation. Toujours est-il que ces recommandations témoignent que la gouvernance des normes reste un chantier politique ouvert, où le débat porte sur le degré de centralisation et la capacité du CNIG à entraîner l'ensemble de l'écosystème. Le CNIG est donc un objet de négociation permanente, entre ministères pour son pilotage d'une part, entre niveau central et échelons territoriaux pour sa déclinaison d'autre part, et plus généralement, entre conception technocratique des normes et ouverture démocratique à un grand nombre d'acteurs.

2.2 Coopérations et conflits entre acteurs nationaux : État, collectivités, agences et secteur privé

L'analyse des rapports de force entre les acteurs de la normalisation des données géographiques en France relève pleinement d'une géopolitique interne, au sens où l'entend Yves Lacoste, c'est-à-dire l'étude des rivalités de pouvoirs sur des territoires[611]. Dans cette perspective, le territoire n'est pas seulement un support passif de l'action publique : il constitue l'enjeu même des conflits entre acteurs institutionnels, économiques et territoriaux qui cherchent à en contrôler la représentation numérique. La donnée géographique, en tant qu'instrument de description et de connaissance du territoire, devient ainsi un vecteur de pouvoir dont la maîtrise conditionne l'exercice de la souveraineté étatique comme les capacités d'action des collectivités locales. Cette section propose d'analyser, à travers le prisme géopolitique, les dynamiques de coopération et de conflit qui structurent l'écosystème français de la normalisation géographique, en portant une attention particulière aux logiques scalaires, aux stratégies d'acteurs et aux enjeux territoriaux qui sous-tendent ces processus.

Sur la scène nationale, le CNIG apparaît comme un microcosme où se côtoient des intérêts institutionnels, économiques et territoriaux. Il regroupe *« des représentants de la très grande variété d'acteurs qui composent l'écosystème de la géodonnée en France : ministères, établissements publics, collectivités territoriales, entreprises privées, associations professionnelles, organisations syndicales, associations de citoyens »*[612], offrant à tous ces acteurs un lieu pour *« se rencontrer, décider et coproduire ensemble »*[613]. Cette composition hétérogène fait du CNIG un véritable microcosme des tensions territoriales françaises, où se confrontent les logiques centralisatrices de l'État et les aspirations

---

610 Ibid.

611 Lacoste Yves, *Dictionnaire de Géopolitique*, Flammarion, 1993. Voir également Subra Philippe, *Géopolitique de l'Aménagement du Territoire*, Armand Colin, 2007.

612 Présentation du site internet du CNIG. Conseil national de l'information géolocalisée. Consulté le 20 janvier 2025.

613 Ibid.

autonomistes des collectivités. Cette ouverture est donc à la fois source de coopération, mais aussi de frictions inhérentes à la diversité des agendas. Ainsi, pour l'État central, l'enjeu est de garantir l'intégration des normes géographiques dans les politiques publiques et la réglementation. Le CNIG, en tant qu'outil à disposition du gouvernement, permet de traduire en standards techniques les priorités nationales. Il s'agit notamment de s'assurer que les données indispensables à l'action publique (urbanisme, risques, biodiversité, infrastructures, etc.) soient disponibles dans des formats interopérables et de qualité homogène sur l'ensemble du territoire. Ainsi, de par la multitude d'acteurs qu'il fédère ainsi que par son autorité confirmée par les statuts du décret du 31 janvier 2011, le CNIG est un pilier de la production de standard et par extensions de données géoréférencées. Les standards CNIG constituent les fondations sur lesquels se repose un nombre grandissant de projets nationaux en matière de production de données géographiques. De fait, les grands projets d'aménagement du territoire à l'échelle nationale se reposent sur la production des standards CNIG, bien que ces derniers puissent parfois précéder la production de certaines données par des acteurs locaux selon des normes conçus et choisis par ces derniers. Le travail du CNIG est donc d'une importance capitale en ce qu'il permet l'harmonisation des productions de données géographiques à l'échelle de l'ensemble du territoire. Le CNIG a également l'avantage d'offrir une plateforme centralisée et reconnue où peuvent se retrouver l'ensemble des acteurs concernés par la production et la gestion de ces données géographiques, ainsi que tous ceux qui sont prêts à s'investir pour aider à leur normalisation. L'existence d'une plateforme telle que le CNIG permet d'assurer un consensus le plus large possible, garantissant à son tour la légitimité des normes ainsi développées et leur large diffusion. Dans cette optique, la France n'hésite pas à donner une force contraignante à certains standards issus du CNIG. Les normes produites par le CNIG revêtent une importance particulière, car, contrairement à la majorité des normes internationales diffusées en France, les normes du CNIG sont souvent soutenues par des lois ou des décrets imposant leurs applications aux acteurs nationaux. Ainsi, aujourd'hui, onze standards du CNIG font l'objet de décrets imposant leurs applications à certains producteurs de données géolocalisées. Cette singularité confère aux normes nationales une portée juridique et donc un véritable poids stratégique, l'État assure ainsi l'exécution de ses directives en matière de données en s'appuyant sur le travail de normalisation du CNIG.

Plusieurs exemples illustrent comment la normalisation sert de relai aux politiques publiques nationales et peut susciter des rapports de force avec les acteurs de terrain. Ainsi, le standard Friches, validé en conseil plénier du CNIG en 2022, a pour but de décrire *« la structure et le contenu des données permettant d'identifier et de caractériser les friches. Il a vocation à être partagé par tous les maîtres d'ouvrage d'inventaires territoriaux de friches qui s'inscriront dans la démarche du Réseau des Inventaires Territoriaux de Friches (RITF). Il permet de donner de la cohérence à ces travaux*

locaux, rendre comparables les données constituées, et leur permettre ainsi des économies d'investissements, facilitant les échanges tant avec Cartofriches qu'avec les acteurs qui s'intégreront dans cet écosystème »[614]. Le décret n° 2023-1259 du 26 décembre 2023[615], qui vise à introduire une définition des friches au sein du code de l'urbanisme, s'appuie sur le standard CNIG pour dresser l'inventaire des friches du territoire. Ce dernier précise ainsi que *« le décret indique que les inventaires conduits par certains acteurs publics ou des agences d'urbanisme sont réalisés notamment d'après les standards du Conseil national de l'information géolocalisée (CNIG) et contribuent à alimenter un inventaire national »*[616]. Ici, le pouvoir réglementaire impose donc aux collectivités et agences d'urbanisme un format commun pour recenser les friches, assurant l'agrégation des données locales à l'échelle du pays. Les collectivités territoriales, obligées de se plier à un schéma national, peuvent y voir une contrainte supplémentaire dictée d'en haut. Un sentiment souvent exprimé par les agents interrogés. Toutefois, le CNIG a veillé à associer ces acteurs en amont dans le groupe de travail "Friches", de sorte que le standard émane d'un consensus professionnel (incluant notamment le Cerema, les agences d'urbanisme, etc.) avant d'être sanctifié par l'État. Le CNIG, par sa structure orientée vers le partage et l'échange entre les différents acteurs impliqués dans l'élaboration et l'application des normes, participe à atténuer les tensions en ouvrant au maximum l'espace des débats durant la conception des standards. De même, le standard « Accessibilité » (cheminements pour personnes à mobilité réduite), publiée la première fois en 2021 et mise à jour en février 2024, a pour but de *« spécifier et standardiser les données utiles au cheminement des personnes à mobilité réduite ou en situation de handicap dans les domaines voirie, espace public, et établissements recevant du public »*[617]. Le décret n° 2021-836 du 29 juin 2021 de la loi LOM, s'appuie sur ce standard concernant la saisie de l'accessibilité des itinéraires pédestres. Il est ainsi indiqué *« En vue d'assurer la collecte de données harmonisées relatives à l'accessibilité des itinéraires mentionnés à l'article R. 141-23, la description d'accessibilité de ces itinéraires s'effectue conformément au standard de données pertinent validé par la structure de coordination nationale prévue par les articles 18 et 19, paragraphe 2, de la directive 2007/2/ CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne »*[618]. En des termes moins abstraits, cela signifie que toutes les collectivités gestionnaires de voirie doivent utiliser le standard

---

614 Cerema, « Standard Friches, Structure de données ouvertes pour inventorier et caractériser les friches », (version 2022 – rev. V2023-12), 2023, p. 6.

615 Décret n° 2023-1259 du 26 décembre 2023 précisant les modalités d'application de la définition de la friche dans le code de l'urbanisme.

616 Décret n° 2023-1259 du 26 décembre 2023 précisant les modalités d'application de la définition de la friche dans le code de l'urbanisme, Introduction.

617 Standard CNIG, « Accessibilité du cheminement en voirie : Collecte des données sur l'accessibilité du cheminement pour les personnes en situation de handicap », (v2021 - rev. Février 2024), 2024, p. 4.

618 Loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités.

CNIG « Accessibilité » pour décrire les cheminements piétons, afin d'assurer l'harmonisation des bases de données dans le domaine des déplacements doux. Là encore, la normalisation devient un outil de mise en œuvre des obligations européennes (INSPIRE) via le prisme national, et un outil de mise en cohérence territoriale, chaque commune devant fournir ses données selon un canevas commun, sous peine de voir ses données inexploitables dans les services nationaux. Si l'objectif d'intérêt général fait consensus, la contrainte normative peut être perçue diversement selon les capacités locales : les grandes villes ou régions, déjà dotées de services SIG performants, y adhèrent plus facilement que de petites communes dépourvues d'ingénierie, pour qui la normalisation représente un défi technique.

Le clivage territorial est, en effet, un aspect crucial. L'examen des processus de normalisation révèle une géographie différenciée des rapports de force, où les caractéristiques territoriales conditionnent la capacité des acteurs à peser sur les décisions. Le clivage centre/périphérie, structurant de l'organisation territoriale française[619], se retrouve dans la fabrique des normes géographiques. Les régions métropolitaines, dotées de services SIG performants et d'une expertise technique consolidée, participent activement aux groupes de travail du CNIG et parviennent à faire entendre leurs spécificités. À l'inverse, les territoires périphériques, ruraux ou ultramarins, peinent à mobiliser les ressources nécessaires pour influencer des processus normatifs qui leur seront pourtant applicables.

Le CNIG évolue dans un contexte où les collectivités ont des niveaux de maturité très hétérogènes vis-à-vis des géodonnées. Certaines régions ou métropoles ont développé tôt leurs propres standards ou bases de données locales, potentiellement divergentes des référentiels nationaux. Par exemple, en matière d'occupation du sol, plusieurs régions s'étaient lancées avant 2014 dans la production d'atlas locaux, avec leurs méthodes et légendes propres. Cette situation a pu créer des frictions territoriales, chaque entité défendant « son » mode de faire. Conscient du risque de morcellement, l'État a missionné le Cerema pour élaborer un guide national OCS GE (Occupation du sol à grande échelle) sous l'égide du CNIG[620]. Le guide OCS GE[621] a été publié le 10 septembre 2014 par le Cerema, dans le but de guider les producteurs de données d'occupation des sols nationaux. En effet, certaines régions ou collectivités locales s'étaient déjà lancées dans la production d'atlas locaux d'occupation des sols. La production du guide OCS GE devait permettre de répondre à la fois aux exigences européennes en la matière depuis le lancement de l'« European Environment Information and Observation Network » (EIONET). Au sein de ce groupe, le groupe de travail EAGLE (Eionet Action Group on Land monitoring in Europe) a cherché à développer de solutions à une meilleure

[619] Sur le modèle centre/périphérie appliqué à la France, voir Gravier Jean-François, *Paris et le désert français*, Le Portulan, 1947 ; et pour une actualisation, Davezies Laurent, *La crise qui vient. La nouvelle fracture territoriale*, Seuil, 2012.

[620] Il est aujourd'hui disponible sur le portail de l'artificialisation des sols ici : Occupation du sol à grande échelle (OCS GE) | Fiche donnée | Portail de l'artificialisation des sols . Consulté le 8 mai 2025.

[621] Prescriptions nationales pour la production des bases de données d'occupation des sols à grande échelle

intégration et à une meilleure harmonisation des activités nationales par rapport aux initiatives européennes de surveillance des terres. Le groupe EAGLE a produit un premier modèle de nomenclature visant à classer les différents modes d'occupation des sols. Le guide OCS GE a été créé afin de garantir une couverture nationale cohérente et dans le respect des directives européennes. Le décret n° 2023-1096 du 27 novembre 2023 relatif à l'évaluation et au suivi de l'artificialisation des sols s'appuie sur le guide OCS GE validé par le CNIG afin de définir la surface des polygones délimitant les différentes zones d'occupation des sols tel qu'indiqué à l'Article 1 *« (…) L'occupation effective est mesurée à l'échelle de polygones dont la surface est définie en fonction de seuils de référence fixés dans la nomenclature annexée au présent article selon les standards du Conseil national de l'information géolocalisée »*[622]. Le CNIG, par ce biais, a joué un rôle de médiateur entre l'échelle européenne qui pousse à l'harmonisation par le haut, et les initiatives régionales qui expriment des besoins de terrain. La publication du guide OCS GE a donc permis de poser un cadre commun, sans immédiatement recourir à la contrainte légale. Il y a donc eu ici une institutionnalisation progressive, d'une incitation technique via un guide CNIG proposé aux producteurs locaux, a émergé un standard de fait, puis une obligation réglementaire intégrée aux politiques d'urbanisme via la loi climat et résilience imposant le suivi de l'artificialisation. Le développement des normes et les relations plus ou moins conflictuelles des acteurs impliqués décrivent ici une géopolitique interne particulière de cette production. Ainsi, l'État, garant de l'unité territoriale et des engagements internationaux (ici, limiter l'artificialisation nette), utilise la normalisation (via CNIG) pour aligner les pratiques locales sur un objectif commun, arbitrant entre la diversité territoriale et l'intérêt national.

Aux côtés de l'État et des collectivités, les agences publiques et opérateurs nationaux, tels que l'IGN, le Cerema, Météo-France, ou encore l'INSEE, jouent un rôle déterminant dans la fabrique des normes et parfois en concurrent les unes avec les autres. L'IGN, producteur de référentiels de base, voit dans la standardisation un moyen d'assurer la fiabilité des données de référence et de conforter son rôle de pivot technique. Cependant, l'IGN ne détient plus le monopole de la donnée géographique, en particulier concernant les normes, depuis le rétablissement du CNIG, d'autres établissements sectoriels possèdent leurs propres bases de données géographiques, comme le ministère de la Transition écologique via ses inventaires naturalistes, ou le ministère de l'Agriculture pour les données foncières. Le CNIG sert de table de négociation pour ces organismes, afin d'éviter des doublons et de convenir de schémas communs. Parfois, il faut aussi composer avec les intérêts économiques d'opérateurs chargés d'une mission de service public. Un cas emblématique est le standard PCRS (Plan Corps de Rue Simplifié), qui définit un référentiel très précis pour les plans de voirie. Ce standard, publié en juin 2015, dresse un référentiel unique à l'échelle du territoire national décrivant les limites de la voirie

[622] Décret n° 2023-1096 du 27 novembre 2023 relatif à l'évaluation et au suivi de l'artificialisation des sols, Article 1.

urbaine. Le PCRS est devenu le fond de plan unique pour l'organisation de tous les travaux de voiries requérant une précision centimétrique. Ce standard a été développé afin de répondre aux exigences de l'arrêté du 15 février 2012 en application du décret DT-DICT[623]. À la suite de la publication du PCRS, l'article 7 de l'arrêté du 15 février 2012 qui se retrouve ainsi modifié : *« 7eme : Le fond de plan employé pour la transmission des données de localisation des réseaux aux déclarants est le meilleur lever régulier à grande échelle disponible, établi et mis à jour par l'autorité publique locale compétente en conformité avec les articles L. 127-1 et suivants du code de l'environnement et selon le format d'échange PCRS (plan corps de rue simplifié) établi et mis à jour par le Conseil national de l'information géographique »*[624]. L'adoption du PCRS comme standard national obligatoire a impliqué de faire collaborer des acteurs parfois rivaux, en rassemblant les collectivités (gestionnaires de voirie), entreprises de travaux, concessionnaires de réseaux (eaux, électricité, télécoms) et services de l'État. Ainsi, le cas du PCRS montre bien que la norme est un compromis technique aux implications économiques. En effet, le PCRS crée un marché pour des prestataires capables de lever ce plan au standard exigé, et oblige à des investissements en cartographie à grande échelle. Ici, le CNIG a été l'arène où ces compromis se sont construits. Le succès du PCRS a encouragé la création d'autres géostandards de réseaux, comme StaR-DT[625] pour les déclarations de travaux, ou encore StaR-Elec pour les réseaux électriques, et ce, toujours sous l'égide du CNIG et en concertation avec les industriels concernés. Chaque nouveau standard sectoriel révèle des négociations entre acteurs aux intérêts

---

623 Articles L. 554-1 à 5 et R. 554-1 à 38 du code de l'environnement, et Arrêté modifié du 15 février 2012 pris en application du chapitre IV du titre V du livre V du code de l'environnement relatif à l'exécution de travaux à proximité de certains ouvrages souterrains, aériens ou subaquatiques de transport ou de distribution.

624 Arrêté du 15 février 2012 pris en application du chapitre IV du titre V du livre V du code de l'environnement relatif à l'exécution de travaux à proximité de certains ouvrages souterrains, aériens ou subaquatiques de transport ou de distribution, article 7.

625 Le StaR-DT (STAndard géographique de Réseaux pour les réponses aux déclarations de Travaux) est un géostandard de description simplifiée des réseaux relevant de la réglementation anti-endommagement, à savoir l'arrêté du 15 février 2012 modifié en application du décret DT-DICT (Décret n° 2011-1241 du 5 octobre 2011 et ses décrets modificatifs). Aujourd'hui le StaRDT constitue le socle commun de base décrivant à très grande échelle les réseaux concernés par le Décret DT-DICT afin de permettre à leurs gestionnaires et aux collectivités concernées d'échanger les informations utiles à la géolocalisation des ouvrages en amont des travaux. Ce sont ces mêmes préoccupations qui ont présidé à la publication du géostandard de réseaux électriques StaR-Elec le 24 novembre 2022. Le StaR-Elec est un géostandard de description métier des réseaux électriques au sens large (transport, distribution, éclairage, signalisation), basé sur le modèle de StaR-DT. Il vise à répondre au besoin de modélisation des ouvrages construits pour les échanges entre acteurs d'un projet (MOA, MOE, entreprise de travaux, topographe, cartographe), à la suite de l'expression de besoin des ouvrages à construire, d'un programme de travaux établi, jusqu'au récolement et l'intégration dans les SI de l'exploitant. De ce fait, il permet de constituer une sorte de jumeau numérique de l'ouvrage, de plus en plus détaillé au fil de son jalonnement. Le StaR-DT constitue le socle commun de base décrivant à très grande échelle les réseaux concernés par le Décret DT-DICT afin de permettre à leurs gestionnaires et aux collectivités concernées d'échanger les informations utiles à la géolocalisation des ouvrages en amont des travaux. La conception du StaR-Elec s'est appuyée le plus possible sur la version 1.0 de StaR-DT. La rédaction des standards StaR-DT et StaR-Elec ayant eu lieu sur une période commune, les objets, attributs et listes de valeurs ont fait l'objet de réunions d'harmonisation entre les deux groupes de travail afin de garantir leur cohérence. Source : Décret n° 2011-1241 du 5 octobre 2011 relatif à l'exécution de travaux à proximité de certains ouvrages souterrains, aériens ou subaquatiques de transport ou de distribution. Disponible ici : Décret n° 2011-1241 du 5 octobre 2011 relatif à l'exécution de travaux à proximité de certains ouvrages souterrains, aériens ou subaquatiques de transport ou de distribution – Légifrance. Consulté le 13 juin 2025.

potentiellement divergents avec, par exemple, les opérateurs d'électricité souhaitant un modèle collant à leurs besoins métier, les collectivités voulant un format simple à gérer, l'État cherchant à réduire les risques et à améliorer l'efficacité globale. La médiation normative opérée par le CNIG permet donc d'aboutir à des schémas validés consensuellement, puis éventuellement rendus obligatoires par la puissance publique, ce qui assure à la fois l'efficacité technique et l'autorité politique de la norme.

Enfin, le secteur privé et économique apporte une autre dimension aux rivalités autour des normes géographiques. D'une part, de nombreuses entreprises utilisent ou produisent des données géolocalisées (bureaux d'études, géomètres, opérateurs de télécommunications, start-ups en géomatique, géants du web, etc.) et sont impactées par les standards. Le fait d'imposer un standard CNIG peut représenter pour elles une contrainte, comme adapter leurs logiciels, ou encore suivre des procédures spécifiques, mais aussi une opportunité économique si elles savent s'en emparer via le développement de nouveaux services de mise en conformité, ou la valorisation de données harmonisées. Le CNIG intègre des représentants du secteur privé et des associations professionnelles pour tenir compte de ces réalités. Par exemple, la commission « Modèles économiques » du CNIG a précisément pour mission de traiter des aspects économiques de la production et diffusion des données. Ces aspects économiques ne sont donc pas négligés par le CNIG, qui a conscience que la normalisation n'est pas qu'une affaire technique, et qu'elle touche aux modèles d'affaires, et aux coûts et bénéfices pour les parties prenantes. Des frictions peuvent surgir si une norme favorise certains acteurs économiques au détriment d'autres. L'exemple de la Base Adresses Nationale en 2015 est ici révélateur. La constitution d'une Base Adresse Nationale ouverte, poussée par l'État et le CNIG, a suscité des tensions avec des entreprises qui commercialisaient jusqu'alors des fichiers d'adresses en concurrence. En ouvrant la donnée selon un standard unifié, le CNIG a participé à rebattre les cartes du marché des données d'adresses en donnant l'avantage aux utilisateurs finaux et aux nouveaux services innovants, mais obligeant certains intermédiaires à se repositionner. De même, l'intégration d'OpenStreetMap France au CNIG signale l'entrée d'un acteur atypique représentant une communauté bénévole produisant une cartographie libre mondiale. Sa présence pourrait influencer les discussions, par exemple en encourageant l'adoption de standards ouverts compatibles avec OSM, ou en posant la question de la dépendance vis-à-vis des plateformes privées (Google Maps en tête) dans l'écosystème français. La dimension économique de la géopolitique de la standardisation nationale est un aspect crucial du développement des normes. Il s'agit ici de garantir des standards ouverts et un écosystème diversifié est un moyen, pour la puissance publique, de ne pas être captif des solutions propriétaires d'entreprises souvent étrangères. C'est un équilibre délicat entre la collaboration public-privé, les deux ayant intérêt à l'interopérabilité, et la confrontation dès lors qu'il s'agit de suprématie sur des pans entiers de la chaîne de valeur de la donnée.

En somme, sur le plan national, le CNIG joue un rôle d'arbitre et de catalyseur dans un paysage où s'entremêlent coopération et conflits latents. Il incarne une forme de gouvernance ouverte des normes en s'efforçant de rassembler toutes les parties prenantes à la table des négociations pour élaborer les standards, ce qui tend à légitimer et faciliter ensuite leur adoption. Toutefois, cette gouvernance collaborative ne doit pas masquer les rapports de force. Ainsi, le cadre légal et la bénédiction de l'État restent souvent nécessaires pour entériner les décisions, et certains acteurs disposent de plus de ressources pour influencer les choix techniques. Le caractère stratégique des normes apparaît dans le fait qu'elles sont intégrées aux lois, qu'elles conditionnent la réussite de politiques nationales, et qu'elles reflètent une volonté de l'État d'asseoir sa souveraineté numérique. À travers le CNIG, la France a mis en place un dispositif lui permettant de maîtriser ses données géographiques tout en associant largement les parties prenantes, afin d'éviter les blocages. Le CNIG est donc un acteur essentiel de la géopolitique interne des normes en France, équilibrer centralisation et pluralisme, uniformité nationale et respect des spécificités locales, impératifs économiques et missions d'intérêt général.

2.3 Les plateformes d'information géographiques en France : un paysage très hétérogène

Étant en charge de la diffusion et de la gestion des informations géographiques régionales et interrégionales, ainsi que dans les grandes agglomérations, les plateformes d'information géographiques présentes sur tout le territoire, constituent un maillon essentiel de la chaîne de production des données géographiques en France. Ces plateformes et leurs gestionnaires sont des acteurs clés de la normalisation des données géographiques. Créées dans le courant des années 90, sous l'impulsion des premières mesures en matière de numérisation des cadastres, elles se sont développées à tous les échelons territoriaux (régions, départements, communautés de communes…) très souvent avec le soutien de l'État. Mettant à disposition des données plurithématique, les plateformes d'informations géographiques sont passées, au fil des années, d'une collecte de données purement géographiques à un éventail très large de données sur les territoires. Ces dernières sont devenues ces vingt dernières années des piliers du développement territorial, en devenant des outils d'aide à la décision cruciaux, en permettant la collecte, l'actualisation, la diffusion et la pérennisation des données territoriales. Elles participent également à développer avec les acteurs concernés des applications spécialisés en fonction des spécificités des territoires et leurs projets. Les organismes en charge de ces plateformes offrent également des outils de mutualisation et d'animation autour des données qu'elles hébergent afin de familiariser l'ensemble des parties prenantes intéressées avec ces données.

Le développement des plateformes d'information géographiques s'explique en grande partie par les initiatives politiques qui se sont multipliées depuis les années 2000 visant à mettre en valeur les données, en particulier celles produites et gérées par les services de l'État. Dès 2003, l'Union européenne publie la directive 2003/98/CE[626] sur les informations du service public, visant à rendre public un maximum d'informations issues des services publics des États membres. En 2011 la création du portail Data.gouv permet la centralisation de l'ensemble des données gouvernementales mises à dispositions des citoyens, informations géographiques comprises. Cette nouvelle politique de la donnée s'est poursuivie avec la publication de la circulaire du 27 avril 2021[627] par le Premier Ministre, suite aux recommandations du rapport Bothorel[628] sur la politique publique de la donnée, des algorithmes et

---

626 Directive2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public. Https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:345:0090:0096:FR:PDF

627 Liste des actions prises par les ministères dans le cadre des feuilles de routes ministérielles, 27 avril 2021. https://www.data.gouv.fr/fr/datasets/liste-des-actions-prises-par-les-ministeres-dans-le-cadre-des-feuilles-de-routes-ministerielles/

628 Rapport sur la politique publique de la donnée, des algorithmes et des codes sources, 23 décembre 2020. https://www.info.gouv.fr/actualite/remise-du-rapport-sur-la-politique-publique-de-la-donnee-des-algorithmes-et-des-codes-sources

des codes sources. Cependant, si des progrès ont été faits en matière d'ouverture de la donnée, cette ouverture seule ne suffit pas à en garantir la réutilisation efficace. Plusieurs enquêtes ont pointé du doigt le besoin d'une gouvernance efficace de la donnée en vue de sa réutilisation afin d'en tirer un véritable bénéfice. À cet égard, l'enquête de l'OCDE de 2020[629] sur la gouvernance des données peut être citée. Elle démontre qu'un travail actif sur les données est nécessaire pour pouvoir en tirer tout leur potentiel au-delà de mise à disposition. À ce titre, le rapport du Conseil d'État sur la réutilisation des données de santé souligne bien également que, si la France dispose d'un vaste patrimoine de données de santé, le manque d'interopérabilité provoque une sous-exploitation de ces bases de données. De plus, malgré l'existence du Health data hub depuis 2019 qui rassemble un grand nombre de bases de données de santé, la manque de confiance de certains acteurs provoque de fortes réticences quant au partage des données[630].

Comme noté dans la première partie de cette thèse, la nouvelle stratégie européenne en matière de donnée va également accélérer le développement des plateformes de données géographiques. La fondation des espaces communs de données (ECD) participe de la structuration de nouveaux espaces de partage de données entre États membres et entreprises privées entre eux et au sein de chaque État. En France le rapport de la députée Faure-Muntian sur les données géographiques souveraines de 2018[631] va aboutir à la création des CRIG (Conseils Régionaux de l'Information Géographique) qui sont les relais du CNIG dans les régions.

La particularité française réside dans le très grand nombre de ces plateformes réparties sur l'ensemble du territoire. Dès 2014, on dénombrait déjà 65 infrastructures de données géographiques se revendiquant comme des "SDI" (Spatial Data Infrastructures), un nombre relativement élevé comparé à d'autres pays européens[632]. Ce chiffre a fortement augmenté au cours de la dernière décennie. D'après l'enquête menée par l'Afigéo de mars à mai 2022[633], les plateformes d'informations géographiques sont aujourd'hui d'environs 130 sur l'ensemble du territoire. Ces dernières se concentrent majoritairement à l'échelle régionale [634] (44%), puis aux échelons départemental (23%), intercommunal (18 %) et enfin national (16%). Avec plus de 10 000 structures bénéficiant de leurs services et près de 265 ETP

---

629 OCDE, « La gouvernance des données dans le secteur public », 2020. https://www.oecd-ilibrary.org/sites/48842dc1-fr/index.html?itemId=/content/component/48842dc1-fr

630 Fauchier-Magnan Emilie (IGAS) et Fradel Julien (Conseil d'État) (rapporteurs), « Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé », Rapport au Conseil d'État, 5 décembre 2023.

631 Faure-Muntian Valéria, « Les données géographiques souveraines - Rapport au Gouvernement », 19 juillet 2018.

632 Jade Georis-Creuseveau1, Christophe Claramunt, Françoise Gourmelon, Bruno Pinaud, et Laurence David, « A Diachronic Perspective on the Use of French Spatial Data Infrastructures », *Journal of Geographic Information System*, 10, pp. 344-361, p. 346., 8 août 2018. https://www.scirp.org/journal/paperinformation?paperid=86528. Consulté le 19 mars 2025.

633 Afigéo, « Les plateformes territoriales de données géographiques : état des lieux, enjeux et perspectives », juin 2023, p. 9.

634 La liste des répondants et les principales informations caractérisant leur plateforme sont accessibles à l'adresse https://docs.google.com/spreadsheets/d/1b1PEvbEVbSBlsuW9Nh0MgBObZa8hcGEd/edit#gid=696507931

(Équivalent Temps Plein) travaillant à leur gestion et à leur animation, la richesse de l'écosystème des plateformes géographiques n'est plus à démontrer. Autrement dit, le tissu français est dominé par des portails régionaux et locaux, un modèle décentralisé qui distingue la France du reste du monde, là où d'autres États ont souvent privilégié une infrastructure nationale centralisée unique[635]. La mise en place dès 2006 du Géoportail national par l'IGN (devenu en 2023 carte.gouv) n'a d'ailleurs pas empêché ce foisonnement d'initiatives locales, reflet d'une forte autonomisation des acteurs territoriaux dans la gestion de leurs données géographiques. Cependant, le paysage des plateformes d'information géographique est marqué par son extrême diversité, avec de grandes disparités entre les régions et les plateformes, en termes de ressources humaines comme de financement. Ainsi, l'effectif moyen est de 4,2 ETP par plateforme, soit 1 ETP pour 377 structures utilisatrices en moyenne. De plus, le manque de moyens humains et financiers qui frappe certaines plateformes rend difficile la mise en place de programmes ambitieux dans certains territoires, et fait parfois obstacle à l'implémentation efficace de certains standards de données. Ainsi, même si des normes obligatoires découlant de l'application de la directive INSPIRE doivent être respectées, celles-ci ne le sont pas toujours dans les différentes plateformes régionales. Ce manque de moyens financiers et humains impacte également les mesures en matière de cybersécurité appliquées à ces plateformes. Certains organismes en manque d'experts informatiques ou en sous-effectifs se reposent sur des processus parfois archaïques de protection, faute de pouvoir faire mieux.

Cette hétérogénéité se retrouve également concernant les formes de gouvernance des plateformes. Ces dernières sont régies par différents statuts juridiques en fonction de leur implantation. Cette diversité de gouvernance empêche parfois la coopération entre certaines plateformes, et peut dans certains cas ralentir le développement de certains projets portés par les plateformes. Ainsi, toujours d'après l'enquête de l'Afigéo de 2022[636], la majorité des plateformes émanent des collectivités territoriales (39%). Certaines ont une gouvernance mixte, mêlant collectivités et État (24%). Certaines sont des associations (19%) ou des établissements publics d'État (18%). Cette diversité de statuts se retrouve également entre les différents acteurs régionaux et départementaux qui participent à la production des données géographiques. Cette diversité reflète les modalités locales d'organisation, mais peut aussi freiner la coopération interrégionale, chaque formule juridique ayant ses limites. Ainsi, la capacité à monter des projets ambitieux diffère selon le statut et les ressources de chaque plateforme. Ainsi, certaines disposent d'un budget dédié, notamment quand elles sont structurées en GIP ou en

---

635 Jade Georis-Creuseveau1, Christophe Claramunt, Françoise Gourmelon, Bruno Pinaud, et Laurence David, « A Diachronic Perspective on the Use of French Spatial Data Infrastructures », *Journal of Geographic Information System*, 10, pp. 344-361, p. 346., 8 août 2018. https://www.scirp.org/journal/paperinformation?paperid=86528. Consulté le 19 mars 2025.

636 Afigéo, « Les plateformes territoriales de données géographiques : état des lieux, enjeux et perspectives », juin 2023, p. 13.

association ouverte aux cofinancements, tandis que d'autres, sans personnalité juridique propre, doivent recréer à chaque fois des montages partenariaux complexes pour financer un nouveau projet. À titre d'exemple, en région Normandie, si la plateforme de donnée GéoNormandie est cofinancée par la région et le département sur la base d'une convention partenariale et financière entre l'État et la région, ce n'est pas le cas de la CRIGE Normandie. Cette dernière ne dispose donc pas de budget propre et son secrétariat relève du financement de la région dans le cadre de la loi Notre. Chaque nouveau projet, comme la production d'un OCS ou d'orthoimages sur le territoire de la région, nécessite de rassembler de nouveaux cofinanceurs. Le manque de budget peut donc faire obstacle aux développements de projets régionaux, là où le statut de GIP (Groupement d'Intérêt Public) pourrait permettre de disposer d'un budget propre. Par extension, la richesse des données mises à disposition sur GéoNormandie pourrait potentiellement s'en trouver amoindri en cas d'absence de financement pour des projets d'acquisition de données. La difficulté principale réside cependant au niveau de la charge et de la gestion administrative des projets. Comme la CRIGE Normandie ne dispose pas de personnalité juridique, elle n'a qu'un seul ETP dédié. Ce qui fait que tout repose sur la bonne volonté des partenaires de la CRIGE. Ainsi, l'absence de structure juridique fait qu'il faut remonter une nouvelle organisation pour chaque montage d'un groupement de commande, ou avance de trésorerie. Il faut à chaque fois repartir de zéro, pour trouver des volontaires, faire un tour de table pour trouver des financements, lancer un groupement de commandes, exécuter le marché, suivre le marché, payer les participants, etc. À l'inverse, en Auvergne–Rhône-Alpes, le CRAIG (Centre Régional Auvergne-Rhône-Alpes de l'Information Géographique) constitué en GIP, ou OpenIG en Occitanie sous statut associatif disposent d'une assise juridique qui leur garantit des contributions régulières de leurs membres et une meilleure continuité dans l'action.

En termes de ressources, les écarts sont également notables. On compte en moyenne seulement 4,2 équivalents temps plein par plateforme (ETP), et certaines ne peuvent dédier qu'un ou deux agents au fonctionnement de leur SIG territorial. Un tel sous-dimensionnement rend difficiles l'implémentation de standards techniques complexes et la conduite de projets innovants dans les territoires moins dotés. En dépit de l'obligation théorique de respecter les normes communes, notamment celles issues de la directive européenne INSPIRE, toutes les plateformes ne parviennent pas à les appliquer pleinement, faute de moyens suffisants. Ce manque de moyens humains et financiers a aussi des incidences directes sur la sécurité et la résilience de ces infrastructures géographiques. Faute d'expertise informatique, certains organismes locaux continuent d'employer des protocoles de protection obsolètes, vulnérables aux cyberattaques, faute de pouvoir faire mieux. Il en résulte une surface d'attaque inégale sur le territoire. Les plateformes les plus fragiles, souvent de petites tailles, peuvent devenir la porte d'entrée de menaces cyber, ce qui pose la question d'une stratégie nationale

cohérente de cybersécurité pour l'ensemble de la chaîne d'information géographique. En effet, les collectivités territoriales sont aujourd'hui des cibles régulières de cyberattaques. Ainsi, l'ANSSI a recensé pas moins de 218 incidents en 2024 rien que sur ce périmètre, soit une moyenne de 18 incidents par mois, pouvant conduire à des interruptions de services ou des vols de données sensibles[637]. Dans ce contexte, l'hétérogénéité des pratiques de sécurité d'une plateforme à l'autre constitue un risque systémique et un enjeu de justice territoriale en matière de protection de l'information. Concernant le financement de ces projets, certains acteurs restent prépondérants, à commencer par les régions et l'État. Ainsi, dans le cas de la Normandie, les acteurs les plus cités sont la Région et l'État ainsi que l'Établissement public foncier de Normandie (EPFN) et les départements[638]. L'IGN et les parcs nationaux sont également des acteurs récurrents des projets portés par les plateformes régionales et les CRIGE. Cependant, tous les projets ne mobilisent pas toujours de financement. À titre d'exemple, les données relatives à l'accessibilité (GT Accessibilité) ainsi que les pistes cyclables (GT vélos) n'ont pas nécessité de montage financier. Ces projets se reposent alors sur la bonne volonté des membres de la CRIGE et le volontariat. Là encore, les disparités régionales se font sentir, et toutes les plateformes ou CRIGEs ne disposent pas du personnel nécessaire pour dégager du temps afin de mener à bien ce type de projets.

Cependant, le partage de données entre les différents acteurs rencontre parfois des difficultés. Ces dernières peuvent être de différentes natures. Il subsiste encore des problèmes d'interopérabilité entre certains jeux de données. Par exemple, le réseau d'observation du littoral normand-Hauts-de-France qui dispose de données de premier plan sur le littoral du nord de la France, gèrent son propre catalogue grâce à un outil développé par Esri et qui n'est pas compatible avec les catalogues de GéoNormandie. Cela amoindrit la visibilité de leur donnée et leur réutilisation[639]. Dans ce contexte le travail effectué par le CNIG prend tout son sens, et contribue grandement par la diffusion des standards de données à atténuer ces effets de « silos » entre différents producteurs de données. Contribuer aux travaux sur la normalisation des données fait partie des missions des différentes plateformes. On peut observer les mêmes disparités concernant la participation des plateformes et des régions aux différents travaux du CNIG. Certains acteurs, tels que l'IGN ou le Cerema participent très activement à ces travaux, tandis que la participation des plateformes est plus disparate. De nouveau, les problèmes de personnels et de moyens tendent à limiter la participation de certaines plateformes aux travaux de normalisation. De même, en fonction des régions, certains besoins sont plus aigus concernant le

---

637 ANSSI, « Collectivités territoriales - Synthèse de la menace », Rapport menaces et incidents du CERT-FR, CERTFR-2025-CTI-002, 24 février 2025. https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-002. Consulté le 12 juillet 2025.

638 Entretien avec le responsable de la CRIGE Normandie, 22 mars 2023.

639 Ibid.

développement de certains standards de données. Cela pousse les plateformes à privilégier la participation à certains groupes de travail dont les standards correspondent plus à leurs besoins spécifiques. Le fait d'orienter les données vers les besoins propres aux régions tend également, sur certaines plateformes, notamment pour certaines métropoles qui disposent de leurs propres plateformes, à mettre à disposition des données uniquement centrées sur leurs besoins propres. Dans certaines régions cela peut provoquer des déséquilibres en matière de mise à disposition de la donnée et accentuer les écarts numériques entre les territoires. Cela entraîne également un potentiel déséquilibre en matière de mise en place de politiques publiques au sein d'une même région ou d'un même département, quand les données sur certains territoires viennent à manquer. In fine, ce déséquilibre informationnel risque d'affecter la capacité à concevoir et appliquer des politiques publiques équitables sur l'ensemble du territoire. Ainsi, les plateformes, initialement pensées pour réduire la disparité d'accès à l'information, pourraient ainsi reproduire malgré elles les inégalités préexistantes si leur développement manque de coordination.

Sur le plan politique et territorial, on assiste donc à des rivalités feutrées entre acteurs institutionnels autour de la gouvernance de ces données stratégiques. D'une part, les collectivités locales, notamment les Régions, ont vu leurs compétences en matière d'information géographique renforcées par la loi NOTRe de 2015[640], qui leur confie explicitement la coordination de la collecte et de la mise à disposition des données de référence sur leur territoire via une plateforme régionale. Les Régions se positionnent ainsi comme des pilotes stratégiques de la politique de l'information géographique, d'autant que les grandes métropoles investissent également ce champ avec des ambitions propres. Ainsi, des villes comme Nice, Bordeaux, Lyon, Rennes, Strasbourg figurent parmi les pionnières. D'autre part, l'État central, historiquement garant des référentiels géodésiques et cartographiques, cherche à maintenir un fil directeur national et la cohérence d'ensemble, surtout face aux enjeux de souveraineté numérique que soulève l'exploitation de la donnée géolocalisée. En effet, comme le souligne un rapport du Sénat, *« les informations qui décrivent le territoire sont des outils stratégiques indispensables à la décision publique. Pour préserver notre autonomie, les données géolocalisées qui fondent nos politiques publiques doivent présenter des garanties d'indépendance. L'emprise des GAFAM sur les géodonnées a rendu cet enjeu plus prégnant encore »*[641]. Autrement dit, il s'agit pour la puissance publique de garder la main sur les données géographiques cruciales, sans

[640] Loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République, NOR : RDFX1412429L, JORF n°0182 du 8 août 2015. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030985460. Consulté le 18 mars 2025.

[641] Vincent Capo-Canellas, « Acteur de référence de la donnée géolocalisée souveraine, l'IGN avance sur un chemin à baliser », Rapport d'information n° 17 (2022-2023), déposé le 5 octobre 2022, p.7. https://www.senat.fr/rap/r22-017/r22-0170.html.

dépendre des grands fournisseurs privés mondiaux, et cela passe par une meilleure coordination de l'écosystème national et l'interopérabilité des systèmes publics.

Les plateformes d'information géographiques constituent la pierre angulaire de la diffusion des données géographiques auprès des citoyens. À ce titre elles occupent une place capitale dans l'écosystème des données géographiques en France, en servant de maillon essentiel entre les acteurs en charge de la capture des données et de leur mise à disposition. Leur grande hétérogénéité en matière de statut juridique et de moyens humain et financier dessine un paysage très contrasté. Cette hétérogénéité se retrouve également dans la nature des données collectées, de leur richesse, et des services qui leur sont associés, là encore du fait de moyens différents. Cependant, un certain nombre de données essentielles se retrouvent sur l'ensemble des plateformes, dans le respect de la directive européenne INSPIRE. C'est en effet par l'imposition de standards européens et nationaux que s'organise la production de données géographiques sur le territoire. Les standards, qu'ils soient obligatoires ou uniquement consultatifs, aident à organiser les données géographiques disponibles et participent à soutenir les politiques publiques d'aménagement du territoire. Les projets nationaux en matière de normalisation des données géographiques sont également le reflet des luttes de pouvoir entre les collectivités et l'État, concernant leur pertinence, les moyens qui leur sont alloués et la répartition des tâches entre les différents acteurs impliqués. En somme, le paysage hétérogène des plateformes géographiques françaises reflète des rapports de pouvoir mouvants entre le centre et la périphérie. Les collectivités revendiquent une part croissante de leadership dans la production et la gestion de l'information géospatiale, forte de leur connaissance du terrain et de l'investissement qu'elles y consacrent. L'État, de son côté, cherche à préserver un cadre unifié garantissant la continuité du territoire national et la maîtrise publique de données critiques. Cette dialectique se traduit par des tensions de gouvernance, notamment concernant les normes à adopter, les investissements à consentir, ou encore le partage des tâches et des financements, mais aussi par des innovations institutionnelles visant à les dépasser, telles que la création d'instances de coopération, comme le CNIG et les CRIG, ou les politiques d'ouverture des données publiques. Elle soulève enfin la question de l'équité territoriale face à la donnée. En effet, comment éviter que la fracture numérique ne se creuse si certaines régions avancent plus vite que d'autres dans l'offre géographique en ligne, ou si les données restent cloisonnées par manque d'interopérabilité ?

En conclusion, l'articulation entre la myriade de plateformes géographiques locales et les projets nationaux de normalisation s'avère un exercice d'équilibrisme permanent, à la fois géopolitique et technique. D'un côté, la France se doit de garantir une cohésion territoriale de l'information géographique, condition de politiques publiques efficaces et équitables, et se doter d'infrastructures résilientes face aux risques cyber comme aux pressions économiques internationales. De l'autre, cette

cohésion ne peut se construire qu'en reconnaissant la montée en puissance des acteurs territoriaux et en intégrant leurs apports et besoins spécifiques. Les rivalités institutionnelles, entre l'État, l'IGN, les agences nationales, les collectivités régionales et locales, sans oublier les instances européennes, ne disparaîtront sans doute pas, car elles traduisent des intérêts et des perspectives parfois divergents. Néanmoins, elles peuvent être canalisées par des mécanismes de gouvernance multiniveaux, une culture du compromis et du partage, comme celle des géocommuns, et par la définition de normes communes servant l'intérêt général. Comme le rappelle l'histoire récente, les périodes de crise ou de transformation, qu'il s'agisse de la révolution des open data, des cybermenaces grandissantes ou des impératifs environnementaux, agissent souvent comme des catalyseurs de changement. Ces dernières obligent les acteurs à coopérer davantage pour surmonter les vulnérabilités collectives. Dans le domaine géospatial, cela se traduit par une double exigence. Tout d'abord, renforcer la standardisation et l'interopérabilité de l'information à toutes les échelles, et enfin veiller à ce qu'aucun territoire ne soit laissé en arrière dans cette montée en compétences. La souveraineté numérique de la France en matière de données géographiques se jouera ainsi dans sa capacité à orchestrer cette mosaïque d'acteurs en un ensemble cohérent, résilient aux crises et innovant, garant de l'indépendance décisionnelle du pays tout en s'ouvrant aux dynamiques collaboratives multiacteurs, qui sont essentiels pour bâtir un tel système en démocratie.

3. Protéger les systèmes d'information militaires à l'heure de la cyberguerre

La guerre du Golfe (1990-1991) est souvent présentée comme le premier conflit de l'ère de l'information. Cependant, il faut toutefois distinguer ce qui relève de la guerre électronique de ce qui relève de la cyberguerre au sens actuel. Ainsi, dès l'ouverture de l'opération Tempête du désert, en janvier 1991, c'est la guerre électronique qui a été mobilisée contre la défense aérienne irakienne[642]. Ce sont John Arquilla et David Ronfeldt qui forgent en 1993 la notion de « cyberwar ». A l'époque, ce terme ne vise pas à décrire ce conflit comme une suite de cyberattaques, les auteurs y voient simplement la démonstration d'une supériorité dans la maîtrise de l'information et du commandement de la part des États-Unis. Selon eux, les États-Unis ont *« fait un travail supérieur en appliquant les principes de la cyberguerre »*, même si ces principes ne sont alors pas encore connus sous ce nom-là[643].

Trois décennies plus tard, cette dépendance à l'information s'est généralisée. Ainsi, dès 2012, le rapport sénatorial de Jean-Marie Bockel constate que les systèmes d'information opérationnelle et de commandement sont *« généralement isolés des autres réseaux »*, mais aussi que *« le nombre croissant de systèmes utilisés et leur interconnexion avec une multitude de terminaux, conformément au principe des opérations en réseaux, élargit le périmètre d'éventuels points de vulnérabilité »*[644]. Le ministère des Armées fait le même constat en 2019. En effet, selon sa politique de lutte informatique défensive, la numérisation des systèmes qui soutiennent son engagement opérationnel, *« via ses systèmes de commandement et ses systèmes d'armes, offre de nouvelles opportunités aux attaquants »*[645]. De plus, sa doctrine de lutte informatique offensive souligne en miroir que celle-ci exploite *« la mise en réseau croissante de l'ensemble des systèmes militaires, ainsi que de leurs interconnexions avec l'Internet »*[646].

---

642 Withington Thomas, « DesertStorm30 – Electric Avenue: Electronic Warfare and the battle against Iraq's air defences during Operation Desert Storm », in *Air Power History*, 20 janvier 2022. https://balloonstodrones.com/2022/01/20/desertstorm30-electric-avenue-electronic-warfare-and-the-battle-against-iraqs-air-defences-during-operation-desert-storm/

643 Arquilla John et Ronfeldt David, « Cyberwar Is Coming! », Comparative Strategy, vol. 12, n° 2, 1993, p. 141-165, repris dans Arquilla John et Ronfeldt David (dir.), In Athena's Camp. Preparing for Conflict in the Information Age, Santa Monica, RAND, 1997, p. 38. https://www.rand.org/pubs/reprints/RP223.html

644 Bockel Jean-Marie, « La cyberdéfense : un enjeu mondial, une priorité nationale », rapport d'information n° 681 (2011-2012) fait au nom de la commission des affaires étrangères, de la défense et des forces armées, Sénat, 18 juillet 2012, p. 31. https://www.senat.fr/rap/r11-681/r11-6811.pdf. Consulté le 15 avril 2025.

645 Ministère des Armées, « Politique ministérielle de lutte informatique défensive », Paris, DICoD, 2019, p. 3. https://www.defense.gouv.fr/sites/default/files/ministere-armees/Politique%20minist%C3%A9rielle%20de%20lutte%20informatique%20d%C3%A9fensive.pdf. Consulté le 15 avril 2025.

646 Ministère des Armées, « Éléments publics de doctrine militaire de lutte informatique offensive », Paris, DICoD, 2019, p. 6. https://www.defense.gouv.fr/sites/default/files/ema/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf Consulté le 2 mars 2025

En France, la numérisation de l'espace de bataille (NEB), engagée dans les années 1990, vise justement à diffuser l'information à tous les échelons, du commandement de la force jusqu'aux unités au contact[647]. L'armée américaine décrit de même son réseau d'entreprise, LandWarNet, comme une infrastructure unique, sécurisée et fondée sur des standards, qui doit relier chaque soldat au même réseau, en garnison comme en opération, au poste de commandement, en mouvement ou en patrouille à pied[648]. Ainsi, dans le domaine des systèmes d'information, notamment géographiques, l'interopérabilité est un principe fondamental qui repose sur des standards communs. A ce titre, comme le note le rapport Bockel, l'emploi d'applications du marché « grand public » dans les systèmes militaires *« augmente elle aussi les risques de vulnérabilité »*[649].

Les communications militaires reposent aujourd'hui sur ce que la doctrine française appelle la couche physique du cyberespace. Cette dernière est faite d' *« ordinateurs, processeurs, câbles, fibres, émetteurs, récepteurs, liens satellitaires, routeurs »*, à laquelle s'ajoutent une couche logique et une couche sémantique (la couche sociale du cyberespace n'entrant pas directement en ligne de compte sur un champ de bataille)[650]. Chacune de ces couches augmentent la surface d'attaque d'un adversaire lors d'un conflit. Ainsi, la couche physique peut être atteinte par la destruction ou le brouillage, la couche logique par l'introduction d'un code malveillant, et la couche sémantique par la manipulation de l'information. L'objectif le plus rentable reste la rupture de la chaîne de commandement. La doctrine française cite d'ailleurs, parmi les emplois possibles de sa propre lutte informatique offensive, la *« neutralisation d'un poste de commandement »* au niveau tactique et la *« neutralisation d'un système de commandement de niveau stratégique »*[651]. Ce qui vaut pour l'adversaire vaut pour les forces françaises. Leur résilience suppose des procédures dégradées, connues et entraînées, qui permettent de poursuivre la mission lorsque les réseaux sont coupés.

A ces éléments s'ajoutent les réseaux militaires qui sont aussi une cible d'espionnage. Ainsi, à partir de 2003, un réseau d'intrusion que les enquêteurs fédéraux américains ont baptisé Titan Rain a pénétré des réseaux sécurisés de bases militaires, d'industriels de défense et d'entreprises aérospatiales. Il a notamment dérobé à l'arsenal de Redstone, siège de l'Army Aviation and Missile Command, le logiciel de planification de vol Falconview utilisé par l'Army et l'Air Force[652]. Les traces de ces

---

[647] Lépinard Philippe et Null Pastorelli Ivan, « Numérisation de l'espace de Bataille : une opportunité pour le développement durable », XVe Conférence AIM, mai 2010. https://hal.science/hal-02133848

[648] US Army, G-3/5/7, « The Army Enterprise Network/LandWarNet », STAND-TO!, 21 juillet 2010. https://www.army.mil/article/42601/the_army_enterprise_networklandwarnet. Consulté le 15 avril 2025.

[649] Ministère des Armées, Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 5.

[650] Ibid., p. 8

[651] Ibid p. 8

[652] Ibid p.9

attaques remontaient vers la province chinoise du Guangdong, bien que le gouvernement chinois ait jugé ces accusations *« totalement infondées »*[653].

Il faut également prendre en compte le fait que de plus en plus de systèmes d'armes contiennent de l'informatique embarqué, ce qui élargit encore la surface d'attaque. Ainsi, en 2009, des insurgés irakiens ont capté, faute de chiffrement, les images transmises par des drones Predator, au moyen d'un logiciel bon marché disponible en ligne[654]. De nouveau en 2011, selon le rapport Bockel, un virus aurait infecté les postes de commande à distance des drones Predator et Reaper après avoir été introduit par des disques durs externes, et un drone américain aurait été détourné au-dessus de l'Iran[655]. Ces cas démontrent que l'accès aux capacités de l'adversaire ne passe pas forcément par le réseau de combat lui-même. Le Ministère de Armées prend très au sérieux cette menace, comme en témoigne par ailleurs la politique ministérielle de 2019, qui résume ainsi ces menaces : *« l'attaquant recherche toujours un point faible ou indirect pour pénétrer les systèmes militaires »*. Le ministère en tire comme conclusion la nécessité d'associer à sa défense les industriels qui développent ces équipements[656].

Avec la popularisation de la navigation par satellite, elle constitue également une autre dépendance critique, en ce que le positionnement des unités, le guidage des munitions et synchronisation horaire des réseaux en dépendent largement. Ainsi, le système Force XXI Battle Command Brigade and Below (FBCB2) de l'US Army, qui repose sur le GPS pour localiser les unités déployées, a été employé lors de l'invasion de l'Irak dès 2003[657]. En 2012, le rapport Bockel rapportait déjà que, selon l'université du Texas, détourner un drone en leurrant ou en brouillant le signal GPS civil coûterait environ 1 000 dollars[658]. Dans le même ordre d'idée, le brouillage est aujourd'hui employé à grande échelle. Sur le front ukrainien, les forces russes brouillent les signaux GNSS, ce qui égare les drones de l'Ukraine, y compris les modèles civils, perturbe la navigation des missiles et contraint l'Ukraine à développer des contre-mesures[659]. Par ailleurs, les États-Unis ont aujourd'hui intégré cette

---

653 Thornburgh Nathan, « The Invasion of the Chinese Cyberspies », TIME, 29 août 2005. https://content.time.com/time/magazine/article/0,9171,1098961,00.html. Consulté le 2 janvier 2025.

654 Jarassé Jim, « Les insurgés irakiens piratent les drones américains », Le Figaro, 17 décembre 2009. https://www.lefigaro.fr/international/2009/12/17/01003-20091217ARTFIG00675-les-insurges-irakiens-piratent-les-drones-americains-.php

655 Bockel, op. cit., p. 31.

656 Ministère des Armées, Politique ministérielle de lutte informatique défensive, op. cit., p. 8.

657 Robb Shane (MAJ), « Force XXI Battle Command Brigade and Below (FBCB2) Past, Present and Future », ARMY AL&T, avril – juin 2007. https://asc.army.mil/docs/pubs/alt/2007/2_AprMayJun/articles/80_Force_XXI_Battle_Command_Brigade_and_Below_%28FBCB2%29_Past%2C_Present_and_Future_200704.pdf Consulté le 23 mars 2025.

658 Bockel, op. cit., p. 75.

659 Slusher Matthew N., « Lessons from the Ukraine Conflict. Modern Warfare in the Age of Autonomy, Information, and Resilience », CSIS, mai 2025, p.3. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-05/250501_Slusher_Ukraine_Conflict.pdf?VersionId=01UUwSkCxsWGAU5vOtwYQHmtq3F1.XKM. Consulté le 12 juin 2025.

dimension dans une doctrine de guerre de la navigation (NAVWAR), qui vise à protéger l'usage du GPS par leurs forces tout en perturbant celui de leurs adversaires[660].

Dans un contexte de numérisation accrue du champ de bataille, la possibilité d'une cyberattaque devient d'autant plus réelle, augmentant les vulnérabilités techniques et humaines des forces dont les opérations s'appuient largement sur ce type de système. Toutefois, toutes les cibles n'ont pas la même valeur. Au contact, détruire un véhicule reste souvent plus simple que d'en pirater les calculateurs[661]. Les cibles les plus intéressantes pour un attaquant se situent plutôt aux niveaux opératif et stratégique : réseaux de théâtre, centres logistiques, liaisons satellitaires et chaînes de commandement, dont la neutralisation peut procurer un avantage durable. Par ailleurs, le ministère des Armées cherche à y répondre par une posture permanente de cyberdéfense, chargée d'assurer *« en permanence (24h/7j) la défense des systèmes informatiques du ministère dans le continuum paix-crise-guerre »*[662]. Il apparaît donc que protéger en priorité les réseaux qui portent le commandement s'impose aujourd'hui comme une priorité pour les forces armées.

3.1 La cyberdéfense dans la doctrine française

La France s'est dotée progressivement depuis le début des années 2010 d'une véritable doctrine en matière de cyberdéfense. Au niveau interministériel, un décret du 11 février 2011 confie à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) la mission d'autorité nationale de défense des systèmes d'information. Quatre jours plus tard, l'agence rend publique une stratégie dont le premier objectif est de *« faire de la France une puissance mondiale de cyberdéfense »*[663]. Cependant, le ministère de la Défense conserve un rôle propre, *« notamment en raison des opérations et des missions à caractère militaire conduites sous l'autorité du chef des armées et dont le cadre d'action ne se limite pas aux zones sous souveraineté nationale »*[664]. A ces deux éléments s'ajoute la Direction générale de l'armement (DGA) qui y contribue également par la maîtrise d'ouvrage des systèmes d'armes et des systèmes d'information militaires, et par son centre Maîtrise de l'information de Bruz, qui réunit alors environ 150 experts[665].

---

660 NAVWAR est une doctrine américaine mise en œuvre via des moyens techniques pour permettre aux forces américaines de protéger leur usage du GPS, tout en perturbant celui de leurs adversaires. Source: https://www.navwar.navy.mil/About/

661 Élodie Simon, Les forces terrestres et le cyberespace comme nouveau champ de bataille, CDEF, 2014

662 Ministère des Armées, Politique ministérielle de lutte informatique défensive, op. cit., p. 9.

663 Bockel, op. cit., p. 75.

664 Ibid., p. 80.

665 Ibid., p. 82

De plus, au sein du ministère, l'organisation fixée par une instruction ministérielle de janvier 2012 distingue deux chaînes. Tout d'abord, il y a la protection des systèmes d'information, qui planifie à moyen et long terme, et qui est animée par le fonctionnaire de sécurité des systèmes d'information. Il y a également leur défense, qui agit en temps réel et qui est commandée par un officier général à la cyberdéfense (OG Cyber), à la tête d'une cellule légère intégrée depuis juillet 2011 à la chaîne de planification et de conduite des opérations[666]. Par ailleurs, Michel Baud précise que l'OG Cyber relève du sous-chef opérations de l'état-major des armées et dispose d'un mandat transverse sur l'ensemble des armées[667]. Placé sous son autorité, le Centre d'analyse en lutte informatique défensive (CALID) surveille les réseaux du ministère et intervient en cas d'incident. Ce dernier travaille avec le centre opérationnel de l'ANSSI, avec lequel sa colocalisation était prévue au second semestre 2013. De plus, un concept et une doctrine interarmées de cyberdéfense ont été adoptés en juillet 2011 et en janvier 2012, sans avoir été rendus publics[668].

Cependant, cette organisation a depuis été refondue. En effet, le Livre blanc de 2013 appelait déjà à une chaîne de cyberdéfense unifiée[669]. Ainsi, le Commandement de la cyberdéfense (COMCYBER), *« créé en mai 2017 par décret »* et placé sous l'autorité directe du chef d'état-major des armées, rassemble désormais l'ensemble des forces de cyberdéfense du ministère[670]. La Revue stratégique de cyberdéfense de février 2018 organise le dispositif national autour de quatre chaînes opérationnelles : « protection », « renseignement », « investigation judiciaire » et « action militaire »[671]. Pour le ministère, la politique de lutte informatique défensive de 2019 décrit une chaîne de commandement « unifiée, centralisée et spécialisée pour tout le ministère ». Ainsi, chaque état-major, direction et service s'appuie sur un centre de supervision de type security operating centre (SOC), en charge du premier niveau de détection. Au-dessus d'eux, le CALID assure une « hypervision » technique d'ensemble, orientée par le centre des opérations cyber du COMCYBER[672]. De plus, le COMCYBER est aussi l'autorité d'emploi de la lutte informatique offensive, qu'il planifie et coordonne au profit de la manœuvre interarmées, du niveau stratégique jusqu'au niveau tactique[673].

Les attaques contre l'Estonie en 2007 puis contre la Géorgie en 2008 ont montré la portée de ces capacités. Ainsi, le 27 avril 2007, une vague d'attaques par déni de service distribué rend indisponibles

---

666 Ibid., p. 80-81
667 Baud Michel, « Cyberguerre. En quête d'une stratégie », Ifri, Focus stratégique n° 44, mai 2013, p. 30. https://www.ifri.org/fr/etudes/cyberguerre-en-quete-dune-strategie Consulté le 18 avril 2025.
668 Bockel, op. cit., p. 81-82.
669 Direction de l'information légale et administrative, « Livre Blanc Défense et Sécurité nationale 2013 », Paris, 2013, p. 94
670 Ministère des Armées, « Commandement de la cyberdéfense (COMCYBER) », site du ministère. https://www.defense.gouv.fr/comcyber/commandement-cyberdefense-comcyber Consulté le 12 février 2025.
671 Ministère des Armées, Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 4.
672 Ministère des Armées, Politique ministérielle de lutte informatique défensive, op. cit., p. 7-8.
673 Ministère des Armées, Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 5 et 7.

jusqu'à 58 sites estoniens en une seule journée et perturbe *« de manière spectaculaire le fonctionnement de la vie courante du pays »*[674]. De même, suite au conflit russo-géorgien d'août 2008, le rapport Bockel conclut que *« l'on ne peut guère concevoir désormais de conflit militaire sans qu'il s'accompagne d'attaques sur les systèmes d'information »*[675]. Aujourd'hui l'omniprésence de l'emploi de ces capacités pose des questions juridiques, notamment concernant les lois entourant les règles d'engagement et le seuil d'agression. Ainsi, en 2019, le ministère des Armées a publié sa lecture du droit international où il affirme que la France intègre *« les principes de distinction, de proportionnalité et de précaution à toute opération de lutte informatique offensive menée en contexte de conflit armé »*[676]. Il est à noter ici que la doctrine française s'écarte du Manuel de Tallinn sur un point notable. En effet, pour la France, une cyberopération constitue une attaque dès lors que les systèmes visés « ne rendent plus le service pour lesquels ils ont été mis en place, que cela soit de manière temporaire ou définitive, réversible ou non » . Cependant, le même texte reconnaît que la majeure partie des cyberopérations françaises en conflit armé, essentiellement de la collecte d'informations, reste en deçà de ce seuil[677]. Il souligne enfin les risques propres à cette arme, liés à *« l'immédiateté de l'action, la dualité des cibles et l'hyperconnectivité des réseaux », une action pouvant « propager ses effets au-delà de la cible visée »*[678].

Enfin, concernant les niveaux d'emploi des forces cyber, la doctrine publique de 2019 en décrit deux. Ainsi, l'emploi de la lutte informatique offensive *« se conçoit aux niveaux stratégique (dans la manœuvre opérationnelle interarmées globale) et tactique (dans la manœuvre des composantes d'armées sur les théâtres d'opération) »*[679]. Elle insiste surtout sur la combinaison des effets : « *Les armées doivent désormais, systématiquement, regarder le combat cybernétique comme un mode d'action à part entière dont les effets se combinent aux autres dans une manœuvre globale »*[680]. Combinée aux modes d'action conventionnels, la lutte informatique offensive devient donc un *« potentiel multiplicateur d'effets »*, capable d'amplifier, d'améliorer ou de compléter leur action[681]. Au niveau tactique, elle est *« une arme dont les effets se combinent à ceux des armes classiques »*[682]. Michel Baud relevait déjà en 2013 que ce milieu « *irrigue l'ensemble des autres domaines (terre, air,*

---

674 Bockel, op. cit., p. 12.
675 Ibid., p. 36.
676 Ministère des Armées, « Droit international appliqué aux opérations dans le cyberespace », Paris, DICoD, 2019, p. 12. https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf. Consulté le 30 septembre 2026.
677 Ibid., p. 13.
678 Ibid., p. 13, et Ministère des Armées, Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 9.
679 Ministère des Armées, Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 7.
680 Ibid, p.4
681 Ibid., p. 6.
682 Ministère des Armées, Droit international appliqué aux opérations dans le cyberespace, op. cit., p. 12.

mer et espace) »[683]. Ainsi, c'est bien la transversalité de la menace cyber qui justifie avant tout la création d'une cyberdéfense véritablement interarmées.

Cette structuration opérationnelle de la cyberdéfense s'accompagne désormais d'une refonte majeure de la gouvernance du numérique au sein du ministère des Armées. La création, par le décret du 6 août 2025, du Commissariat au numérique de défense (CND)[684] marque une rupture institutionnelle significative. Opérationnel depuis le 1er septembre 2025, ce nouvel organisme est placé directement sous l'autorité du ministre des Armées[685]. Sa création répond à un constat formulé par le ministre Sébastien Lecornu : la sédimentation successive des réformes numériques depuis plus de vingt ans avait engendré une organisation fragmentée, manquant de lisibilité et d'efficacité face aux exigences de réactivité qu'impose le contexte stratégique contemporain[686].

Le CND procède de la fusion de trois entités jusqu'alors distinctes : la Direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI)[687], créée en 2004 et chargée des fonctions d'opérateur de télécommunications, la Direction générale du numérique (DGNUM)[688], instituée en 2018 pour piloter la transformation numérique, et l'Agence du numérique de défense (AND)[689], établie en 2021 pour professionnaliser la conduite des projets. L'Agence ministérielle pour l'intelligence artificielle de Défense (AMIAD)[690], créée en 2024, rejoindra le CND en 2026, parachevant ainsi l'unification des capacités numériques du ministère. Cette concentration des moyens et des compétences vise à éliminer les redondances et à garantir une cohérence technique et opérationnelle que la dispersion antérieure rendait difficile à atteindre[691].

D'un point de vue géopolitique, la création du CND s'inscrit dans une logique de renforcement de la souveraineté numérique française. La Loi de programmation militaire 2024-2030 consacre une

---

683 Baud, op. cit., p. 35.

684 Décret n° 2025-782 du 6 août 2025 portant création du Commissariat au numérique de défense, JORF n° 0183 du 8 août 2025.

685 Ministère des Armées, « Présentation du Commissariat au Numérique de Défense », defense.gouv.fr, consulté le 22 janvier 2026. URL : https://www.defense.gouv.fr/cnd/mieux-nous-connaitre/presentation-du-commissariat-au-numerique-defense

686 Lettre du ministre des Armées Sébastien Lecornu, 3 décembre 2024, citée par L'Informé, 24 décembre 2024. Le ministre y évoque le fait que « depuis plus de 20 ans, les réformes du numérique au sein du ministère se sont sédimentées en couches successives. Un décalage de plus en plus grand s'est ainsi créé entre une organisation qui a perdu en lisibilité et en efficacité et le besoin de réactivité et d'agilité ».

687 La DIRISI (Direction interarmées des réseaux d'infrastructure et des systèmes d'information) a été créée le 1er janvier 2004 par décret du 31 décembre 2003. Elle assurait les fonctions d'opérateur de télécommunications et de garant de la sécurité des systèmes d'information du ministère des Armées.

688 La DGNUM (Direction générale du numérique) s'est substituée à la Direction générale des systèmes d'information et de communication (DGSIC) en 2018, avec pour mission de piloter la transformation numérique du ministère.

689 L'AND (Agence du numérique de défense) a été créée en 2021 pour professionnaliser la conduite des projets numériques au sein du ministère.

690 L'AMIAD (Agence ministérielle pour l'intelligence artificielle de Défense) a été créée en 2024 pour aborder les enjeux spécifiques liés à l'intelligence artificielle et à la valorisation des données dans le domaine de la défense.

691 Le général de corps d'armée Erwan Rolland, ancien directeur central de la DIRISI, a été nommé premier commissaire au numérique de défense par décision du Conseil des ministres du 27 août 2025. Il est secondé par l'ingénieur général hors classe de l'armement Lionel Morin, nommé commissaire adjoint.

enveloppe de 20 milliards d'euros au numérique[692], témoignant de l'importance stratégique accordée à ce domaine. Le CND se voit confier la mission de « construire un socle de compétences régaliennes internes » permettant au ministère de *« concevoir, sécuriser et défendre ses systèmes critiques sans dépendre d'acteurs extérieurs »*[693]. Cette ambition de souveraineté se traduit par le développement d'infrastructures souveraines, garantissant la maîtrise des flux sensibles et la robustesse des architectures, y compris pour les transmissions nucléaires. Fait notable, les services de renseignement (DGSE, DRM, DRSD) conservent leur autonomie numérique et ne sont pas intégrés au CND, préservant ainsi l'indépendance de leurs systèmes d'information les plus sensibles[694].

Il faut également distinguer les missions du CND de celles du Commandement de la cyberdéfense (COMCYBER), avec lequel il entretient une relation de complémentarité. Tandis que le COMCYBER, créé en 2017, assume la responsabilité des opérations militaires dans le cyberespace, le CND se concentre quant à lui sur l'infrastructure numérique, la transformation digitale et la gestion des données. Le CND assure ainsi le fonctionnement continu des systèmes numériques et de communication nécessaires aux opérations militaires, tandis que le COMCYBER les défend contre les cybermenaces. Cette articulation institutionnelle, qui « casse les silos pour gagner en agilité »[695] selon les termes du général Erwan Rolland, premier commissaire au numérique de défense, reflète la prise de conscience que la supériorité informationnelle ne peut s'obtenir que par une gouvernance unifiée des moyens numériques, depuis leur conception jusqu'à leur défense en passant par leur exploitation opérationnelle.

Avec le développement des réseaux de communication militaires et l’évolution de la menace cyber, les données géographiques sont aujourd’hui rentrées dans le spectre des données potentiellement impactées par des attaques cyber en temps de guerre. À ce titre, les normes en matière de données géographiques et celles concernant les réseaux de communication se développent aujourd’hui de plus en plus conjointement afin de répondre aux besoins des opérationnels.

Au sein des armées françaises, la standardisation des données géographiques est gérée par plusieurs entités en charge de la coordination entre les industriels de l’armement et les opérationnels. L’une des structures les plus actives est GEOCAPI, qui a renforcé son rôle au cours de l’opération

---

692 La Loi de programmation militaire 2024-2030 prévoit une enveloppe de 20 milliards d'euros consacrée au numérique, témoignant de l'importance stratégique accordée à ce domaine. Voir Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030.

693 Ministère des Armées, « Présentation du Commissariat au Numérique de Défense », *op. cit*. Le site officiel précise que « le CND inscrit son action dans une ambition stratégique forte : renforcer la souveraineté numérique du ministère des Armées pour garantir sa résilience face aux menaces croissantes ».

694 Les services de renseignement (DGSE, DRM, DRSD) conservent leur autonomie numérique et ne sont pas intégrés au CND, signe du caractère stratégique de leur indépendance en matière de systèmes d'information.

695 Entretien du général Erwan Rolland avec *Républik IT*, 28 octobre 2025. Le général y déclare : « En fusionnant [les trois organismes] et en plaçant le CND sous l'autorité directe du Ministre, nous avons cassé les silos pour gagner en agilité ».

Barkhane (2014–2022) en Afrique sahélienne, en s'assurant que les données géographiques produites par l'armée de Terre, la DGA et les industriels soient interopérables et adaptées aux réalités du terrain[696]. Cette opération, marquée par la complexité des environnements désertiques et l'importance de la mobilité tactique, a nécessité la production de données topographiques précises, régulièrement mises à jour et compatibles avec les systèmes de commandement numérisés. GEOCAPI a ainsi joué un rôle stratégique dans l'harmonisation des formats et dans le soutien cartographique déployé sur les théâtres d'opérations. Certains de ces experts sont en permanence déployés sur le porte-avion Charles de Gaulle [697].

Du fait de la disparité des systèmes d'armes et des besoins exprimés par les opérationnels, le choix d'imposer un seul logiciel pour le déploiement de données géographiques au sein ne serait-ce que d'une seule branche de l'armée, comme l'armée de Terre, est impossible. De ce fait, toute la production géographique militaire tourne autour de choix de normes qui permettent d'assurer l'interopérabilité de différents systèmes d'armes et de leurs logiciels embarqués. Ce qui permet également de ne pas dépendre d'un seul producteur de logiciels, comme cela a été souligné auparavant. On s'efforce également de s'assurer que les normes soient à la fois françaises et internationales pour les déploiements en coalition. À titre d'exemple, les données produites dans le cadre du programme Geomaps liant les industriels Thales et Airbus à l'armée de Terre, pour la production de données géographiques, les données produites sont conçues sur la base de normes arrêtées durant des réunions internationales afin de disposer d'un système interallié unifié. Ainsi, en termes de données raster, des standards tels que l'ASRP et l'USRP[698] ont été conçus par le DGIWG. Aujourd'hui ils sont progressivement remplacés par des formats civils plus aisés à manipuler, tels que le JPEG2000[699] ou le GeoTIFF[700]. Concernant les données vecteurs, ces dernières restent assez peu exploitées au sein des armées. Elles servent souvent de base pour concevoir des données rasters, mais il existe peu de systèmes capables de requêter efficacement les données vecteurs et d'en exploiter tout le potentiel. Cette situation aboutit souvent à ce que les produits cartographiques soient fournis aux armées pré-

---

696 Becht Olivier et Gassilloud Thomas, « Rapport d'Information déposé par la Commission de la Défense Nationale et des Forces Armées en conclusion des travaux d'une mission d'information sur les enjeux de la numérisation des armées », Assemblée Nationale, 30 mai 2018. https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b0996_rapport-information. Consulté le 22 mai 2025.

697 Entretien avec le directeur de GEOCAPI, 28 mars 2023.

698 Les produits raster ASRP (ARC Standard Raster Product) et USRP (UTM/UPS Standardized Raster Product), sont des variations d'un format de produit standard commun. Les produits ASRP (dans un système de coordonnées géographiques) et USRP (dans un système de coordonnées UTM/UPS) sont des images à bande unique avec palette et géoréférencement. Ils sont conforme à la norme ISO/IEC 8211 créé en 1994. Source : https://docs.safe.com/fme/html/FME-Form-Documentation/FME-ReadersWriters/asrp/asrp.htm

699 Le JPEG2000 (développé par le Joint Photographic Experts Group) est une norme de compression d'images utilisant une transformée en ondelettes. Source : https://geoservices.ign.fr/sites/default/files/2023-11/DT_JPEG2000.pdf

700 Le Tag(ged) Image File Format, abrégé TIFF, est un format de fichier pour image numérique. Le format GeoTIFF contient, en plus, des informations de géoréférencement dans l'entête de l'image. Source : https://geoservices.ign.fr/actualites/2022-01-13-scan-geotiff

calculés, par exemple en mettant en évidence les bâtiments d'une certaine hauteur sur les cartes. De plus, il n'existe pas de norme internationale multi-logiciel qui permette de faire de la symbologie. Si la norme SLD[701] existe, elle n'est pas toujours suffisante pour répondre à tous les besoins. Par exemple, SLD n'est pas capable de classer les couches de données avant leur affichage. Il se contente de lier un objet à une symbologie, ce qui demande un travail supplémentaire pour organiser les éléments de symbologie de la façon souhaitée, même une fois la carte préparée. Dans l'idéal il faudrait que tout soit normalisé, du vecteur à l'image final, mais une telle solution n'existe pas à l'heure actuelle. Si la société Mapbox[702] propose, par exemple, des produits prêts à l'emploi avec une symbologie normalisée, cela ne répond pas toujours au besoin des utilisateurs, sans lever le problème de la dépendance à une société étrangère.

Une des difficultés propres aux armées quant à l'adoption de norme, provient du cycle très long de production des systèmes d'armes. Ces derniers, non seulement prennent en moyenne entre 10 et 20 ans à être conçus et à entrer en service[703], mais sont également maintenus pendant de longues années, et ne peuvent pas toujours supporter le cycle des mises à jour que certaines normes subissent, nécessitant souvent le maintien en fonctionnement de systèmes qui ne sont pas toujours adaptés aux dernières évolutions en matière de technologie. Les normes en matière de données géographiques tendant à suivre autant que faire se peut les changements de technologies pour s'adapter aux besoins de leurs utilisateurs, ces dernières suivent des cycles de production et d'évolution qui ne sont pas adaptés au rythme de vie beaucoup plus lent des systèmes militaires. Par exemple, le format RPF qui permet l'affichage de carte dans les avions, a été abandonné au début des années 2000, mais reste encore utilisé dans les armées parce que certains avions l'emploient toujours. Dans le cas des données géographiques, cette situation est aggravée non seulement par le rythme soutenu des mises à jour qu'elles peuvent subir, mais également par le fait que la cartographie dispose rarement d'un poids suffisant pour influencer les décisions concernant les choix de technologie ou de normes prises au sein des armées. D'une manière générale on observe une adoption de plus en plus large de normes civiles en matière de production de données géographiques, au détriment de normes spécifiquement militaires afin de faciliter les échanges technologiques entre les technologies civiles et militaires.

Le choix des normes dépend également de l'usage final qui sera fait de la donnée produite selon ce format, qu'il s'agisse de données vecteurs ou raster. Là encore, une problématique spécifique aux

---

701 La norme OGC Styled Layer Descriptor (SLD) définit un encodage qui étend la norme WMS (Web Map Service) pour permettre la symbolisation et la coloration définies par l'utilisateur d'entités géographiques et de données de couverture. Source : https://www.ogc.org/fr/publications/standard/sld/

702 Mapbox est une entreprise américaine spécialisée dans la cartographie en ligne. Source : https://www.mapbox.com/company

703 Cour des Comptes, « La loi de Programmation Militaire (LPM) 2019 – 2025 et les Capacités des Armées », Rapport Publique Thématique, mai 2022, p. 57. https://www.ccomptes.fr/system/files/2022-05/20220511-rapport-bilan-loi-programmation-militaire.pdf. Consulté le 18 juin 2025.

armées se pose, celle de la disparité entre les utilisateurs finaux des données et les spécialistes qui participent aux réunions internationales de normalisation et qui conseillent les armées sur les normes en développement. La majorité des spécialistes en normalisation sont des civils et ces derniers ne sont pas en contact direct avec les militaires. S'il y a bien des retours et une coopération entre les armées et les IGN, ainsi que la DGA, tous les spécialistes ne connaissent pas nécessairement la façon dont les produits cartographiques seront utilisés, ce qui pousse les spécialistes à proposer des standards génériques issus d'organisations comme l'OGC sans connaître nécessairement l'emploi qui en sera fait sur les théâtres d'opérations. Ainsi, il arrive que des normes développées dans le domaine civil nécessitent de nombreux ajustements afin de pouvoir bénéficier efficacement aux armées. Ainsi, les systèmes géospatiaux militaires nécessitent souvent des fonctionnalités allégées, rapides en réseau intermittent, ce pour quoi les standards civils trop complets (géodatabases complexes, métadonnées très détaillées) sont inadaptés, comme le soulignait déjà en 2019 la société Hexagon spécialisée dans le fourniture de services géospatiaux aux armées[704].

À ces problématiques s'ajoute celle liée aux spécificités des systèmes embarqués au sein des systèmes d'armes employés dans toutes les armes. La majorité de la production de ces systèmes d'armes étant sous-traités à des industriels, il arrive que ces derniers ne se rendent pas compte de l'ampleur de la tâche pour afficher les données géographiques nécessaires au sein des systèmes qu'ils développent. Ainsi, lorsque la production d'un nouveau véhicule est lancée, les premières discussions s'engagent entre la DGA et les industriels autour des aspects clés du système d'armes : blindage, capacité d'emport, tout terrain, armement… Ensuite, seulement la question des données géographiques embarquée est abordée : GPS, affichage d'informations tactiques… et certaines exigences en matière de cartographie sont précisés, telles que les coupes terrain, inter-visibilité (d'où peut-on voir et/ou être vu). Cependant, les industriels ne connaissent pas nécessairement les produits cartographiques employés au sein des armées et les normes appliquées. GEOCAPI est alors sollicité pour définir le cahier des charges en matière de cartographie et de fournir des spécifications afin de permettre au système d'embarquer les données requises et respectant les normes choisit. Puisque toutes les données disponibles ne peuvent être embarquées dans le véhicule, un certain nombre d'exigences sont précises aux préalables, tels que le module d'intégration ou la fonction de déplacement sur la carte. Certaines grandes exigences sont cependant indispensables. Ainsi, tous les systèmes d'affichages doivent pouvoir marcher en tout point sur la Terre. Cela n'est pas testable systématiquement durant la phase de production, et, par le passé, certains systèmes d'armes se sont retrouvés inopérables dans l'hémisphère sud, car cette spécification n'avait pas été proprement testée. Ces exigences sont rassemblées dans le

[704] HEXAGON, « END-TO-END GEOSPATIAL SOLUTIONS FOR MILITARY LAND C2 OPERATIONS », White Paper, 15 avril 2019.

document unique du besoin (DUB) qui est transmis aux industriels. Certains systèmes amènent également au développement de logiciels spécifiques qui ne se retrouvent pas dans le civil, comme des logiciels de tir qui nécessitent d'afficher non seulement l'image, mais également des mesures d'altitude, de précision et de coordonnées afin de s'assurer que la source peut être utilisée pour tirer. À titre d'exemple, une donnée cartographique dont la précision est inférieure à six mètres ne peut être utilisée pour coordonner un tir d'artillerie.

Il existe également des exigences spécifiques aux missiles qui fonctionnent sur des modèles de cible. Ces derniers permettent de définir la phase de vol en s'appuyant sur des MNT. Une fois les données MNT chargées en entrée dans le missile, ce dernier va disposer de la forme du sol par radar et il va pouvoir s'orienter sans avoir recours à des signaux GPS qui peuvent être brouillés. C'est par exemple, le principe du TERCOM (Terrain Contour Matching), utilisé dans le missile SCALP-EG français. Ces systèmes requièrent des modèles très précis de la topographie, compatibles avec les capteurs et l'informatique embarquée. De même les aéronefs ont des exigences spécifiques. Les données géographiques doivent être embarquées dans un format optimisé à leurs besoins. Ce format est généralement imaginé par le constructeur de l'avion. Les informations relatives aux normes en vigueur sont communiquées aux industriels, mais seuls eux savent comment ils peuvent incorporer la donnée, mais ils ne savent pas toujours sous quelle forme les produits cartographiques existent. La communication entre industriels et fournisseur de la donnée est toujours essentielle. C'est ici que le rôle des experts de GEOCAPI devient crucial, en permettant d'aider les ingénieurs de la DGA à spécifier les modèles cartographiques adéquats pour vérifier que la donnée utilisée représente bien l'espace souhaité et soit bien géoréférencée. Ils permettent d'aider à comprendre ce que sont réellement les données géographiques, en listant les formats qui existent, notamment dans les programmes de coproduction internationaux. Des spécifications sont écrites, mais restent toujours interprétables. Les industriels ne disposent souvent pas d'experts en données géographiques, ce qui les pousse à sous-traiter ce pan de la production à des experts, mais ces derniers ne participent pas toujours à l'ensemble du cycle de production, ce qui aboutir à des situations de tension où, en cas de manquement, les industriels refusent parfois de reconnaître leurs erreurs après s'être rendu compte qu'ils n'avaient plus accès à leurs experts anciennement engagés sur le programme.

Un autre élément à prendre en compte, lié à la normalisation de ces données dédiées aux armées, est leur qualité. Si normaliser la donnée peut permettre de garantir un certain niveau de qualité, via certaines spécifications, cela n'est pas suffisant. Ainsi, toutes les données satellitaires ont forcément une erreur de localisation, et toutes les données de la défense doivent être qualifiées afin de pouvoir renseigner immédiatement l'utilisateur sur la marge d'erreur à laquelle il doit s'attendre en manipulant la donnée. La date de prise de vue est également importante, car les images satellites sont souvent des

patchworks d'images multiples acquises à différentes dates et qui disposent chacune d'une source. Les métadonnées textuelles qui accompagnent les données permettent de transmettre des informations, sur la conformité des spécifications, la zone couverte, la version de la donnée, la date et permettent le catalogage de la donnée. Ces informations font partie intégrante de la qualité de la donnée.

Comme nous l'avons souligné, la cyberdéfense occupe aujourd'hui une place importante au sein de la doctrine française de défense. L'ensemble des systèmes d'information transmettant des données à distance peuvent faire l'objet d'interférences. La doctrine française en matière de cyberdéfense pour les armées s'appuie également sur les évolutions récentes en matière d'infovalorisation au sein des armées occidentales. Les États-Unis ont été les premiers à concevoir la guerre centrée sur les réseaux (Network Centric Warfare), en plaçant les réseaux de communication et l'avantage informationnel au cœur de leur nouvelle vision du champ de bataille. Cette doctrine, qui a participé à façonner la vision occidentale de la guerre, demande d'être analysée et comprise afin de saisir l'importance des données de toute nature pour la conduite de la guerre au XXIe siècle.

3.2. Émergence du concept de guerre centrée sur les réseaux (Network Centric Warfare) et intégration de la dimension cybernétique dans la doctrine militaire américaine

Comme évoqué dans notre premier chapitre, le concept de guerre axée sur le réseau, également connue sous le nom de Network Centric Warfare (NCW), a été développé par la Révolution dans les Affaires Militaires (RMA)[705]. Ce modèle théorise les conflits dans un environnement cybernétique en réseau, où l'adversaire est perçu comme un nœud au sein d'un réseau. L'idée centrale étant qu'en ciblant les nœuds essentiels de ce réseau adverse, on peut neutraliser l'ennemi en désorganisant ses structures, le rendant ainsi inapte à agir en raison de sa forte dépendance aux systèmes d'information. Depuis la seconde moitié des années 1990, les forces militaires américaines ont commencé à explorer le concept de guerre centrée sur les réseaux (NCW) dans le but d'optimiser la transmission d'informations entre leurs différents services. Cela a permis de rationaliser la prise de décision et d'améliorer leur efficacité sur le champ de bataille. Ce concept est fondé sur des technologies interconnectées via MILNET, le réseau mondial de télécommunications militaires américaines. L'objectif principal du NCW est d'atteindre une supériorité informationnelle, en intégrant sept fonctions essentielles : commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance (C4ISR). En optimisant ces capacités, l'objectif est de mieux gérer l'incertitude en garantissant une supériorité technologique, assurant ainsi la supériorité opérationnelle de la force. Le NCW s'articule autour de trois principes clés : l'objectif constant est de récolter des informations sur les structures et les données des systèmes adverses. Lorsqu'une action est décidée, les cyberattaques ciblent en priorité les systèmes de commandement et de navigation. Par la suite, les attaques s'étendent aux bases organisationnelles de l'ennemi, à sa logistique, à ses soutiens, ainsi qu'à ses infrastructures d'information. Bien que le concept de guerre centrée sur les réseaux ait suscité un vif intérêt au début des années 2000, notamment dans un contexte où les sociétés civiles espéraient des conflits sans pertes humaines, ses limites sont rapidement apparues. La maîtrise complète du champ informationnel et électromagnétique s'est avérée impossible, et la prise de décision en situation d'incertitude demeure une réalité incontournable de l'action militaire. En 2011, l'US Army a publié un plan définissant la cyberguerre comme une composante stratégique pour la période 2016-2028[706]. Ce programme repose sur deux principes fondamentaux :

Le premier affirme que, pour dominer le domaine cyber-électronique, il faut obtenir l'avantage, le sécuriser, et placer les adversaires dans une position défavorable. Le second impose aux chefs

[705] Cebrowski Arthur K., et Garstka John H., « Network-Centric Warfare - Its Origin and Future », Proceedings, Vol. 124, janvier 1998.

[706] US Department of Defense, « Department of Defense Strategy for Operating in Cyberspace », juin 2011. https://csrc.nist.gov/presentations/2011/department-of-defense-strategy-for-operating-in-cy

militaires de préserver leur liberté d'action dans le cyberespace et le champ électromagnétique, tout en privant leurs opposants de cette liberté. Cette capacité d'agir dans le cyberespace est envisagée comme un multiplicateur de forces, facilitant les opérations dans les domaines terrestres, aériens, maritimes et spatiaux.

Les activités américaines dans le cyberespace, désignées par l'appellation *computer network operations* (CNO), se concentrent sur trois axes principaux : la défense, l'attaque, et l'exploitation. La défense des réseaux consiste à prévenir les intrusions dans leurs propres systèmes. L'attaque des réseaux vise à pénétrer les systèmes adverses pour identifier leurs failles et mener des actions qui interrompent, altèrent ou détruisent des informations. L'exploitation des réseaux consiste à tirer parti des informations recueillies dans les systèmes adverses. Ces attaques cybernétiques peuvent être utilisées pour déstabiliser la société civile d'une nation cible ou perturber son efficacité militaire. Certains auteurs utilisent le terme *information and infrastructure operations* (I2OS) pour désigner ces actions visant à semer la confusion, démoraliser, distraire l'adversaire et affaiblir sa capacité de réponse. Les opérations dans le cyberespace, appelées CyberOps, s'inscrivent dans un cadre plus large incluant des activités militaires visant à contrôler le spectre électromagnétique, même en période de paix. Ce cadre repose sur quatre composantes : la guerre cybernétique (CyberWar), les opérations sur réseaux (CyberNetOps), le soutien cybernétique (CyberSpt) et la cyber *situational awareness* (CyberSA)[707].

Ainsi, l'essor des opérations dans le cyberespace témoigne d'une transformation profonde des stratégies militaires, où le contrôle de l'information et des réseaux devient un élément clé du rapport de force entre adversaires. Cette évolution ne se limite pas au domaine numérique, mais s'intègre pleinement aux transformations plus larges du combat moderne. La numérisation du champ de bataille et l'interconnexion des forces combattantes apparaissent aujourd'hui comme les prolongements naturels de ces stratégies cybernétiques, donnant naissance à des concepts tels que la Bulle opérationnelle aéroterrestre en France ou le Network Centric Warfare aux États-Unis. En combinant cybersécurité, renseignement et interopérabilité des systèmes d'armes, ces approches redéfinissent la manière dont les opérations militaires sont planifiées et exécutées, rendant plus crucial que jamais le contrôle des flux d'informations sur les théâtres d'opérations modernes.

[707] *Ibid*

3.3 Les normes au cœur des nouvelles infrastructures de données numériques pour les armées (Integrated Sensor Architecture)

Avec l'émergence du concept de Bulle opérationnelle aéroterrestre et de Numérisation de l'espace de bataille au sein des armées françaises ou encore de celui de Common Operational Picture et Network Centric Warfare au sein de l'armée américaine, l'interconnexion de l'ensemble du personnel combattant devient un objectif majeur du combat futur pour les armées occidentales [708]. Conceptualisée en 1998 par le Vice-Amiral Arthur K. Cebrowski et John Garstka dans la revue Proceedings de l'US Naval Institute dans l'article « Network-Centric Warfare: Its Origins and Future », et mis en pratique pour la première fois durant l'opération « Iraqi Freedom » en 2003[709], cette interconnexion est également une composante essentielle du combat infovalorisé, concept clé des évolutions en matière de tactique entamé par l'armée française depuis les années 2010[710]. La mise en place de la bulle opérationnelle aéroterrestre repose sur la mise en réseau des hommes et des matériels par le biais de systèmes de systèmes (SdS) implémentés à l'ensemble des systèmes d'armes existants modernisés (véhicules blindés, char Leclerc, systèmes SCORPION pour les fantassins…) et ceux en cours de développement (missile de combat terrestre, SCAF…). La mise en place de la bulle opérationnelle aéroterrestre nécessite la maîtrise de capteurs multispectraux (optiques, lasers, radars…) très large et la diffusion d'un ensemble de données hétéroclites (audios, vidéos, images…)[711]. Ces données sont diffusées aux opérationnels par le biais de systèmes d'information interconnectés destinés à décupler la synergie des unités engagées, en s'appuyant sur la complémentarité des différents matériels (blindés, aviation, drones, navires…)[712]. La mise en place de ces systèmes englobants en matière de communication et de partage de données vise également à repenser la façon dont les systèmes d'armes sont développés afin de réduire les coûts et les dépassements de calendrier, en intégrant dès la conception des nouveaux équipements l'intégration de ce dernier à une architecture de capteurs interconnectés.

Au sein de ces systèmes interconnectés, les données géographiques jouent un rôle essentiel. Ces dernières fournissent le socle de toutes les données diffusées qui se doivent d'être géolocalisables afin

---

708 Barraco Laurent, « La bulle opérationnelle aéroterrestre », La Jaune et la Rouge, n° 615, mai 2006.

709 Poduval Sanjay, AIR POWER Journal Vol. 4 No. 2, été 2009, p. 80. https://capsindia.org/wp-content/uploads/2022/10/Sanjay-Poduval.pdf?. Consulté le 5 avril 2025.

710 Boyer Nathalie, « Artist, première expérimentation de la bulle opérationnelle aéroterrestre », DGA, 26 juin 2010. https://archives.defense.gouv.fr/dga/actualite-dga/2009/artist-premiere-experimentation-de-la-bulle-operationnelle-aeroterrestre.html?

711 Imbert Vincent, « La bulle opérationnelle aéroterrestre (BOA) : un choix nécessaire », RDN, n°643, juin 2022, pp. 97 – 106.

712 Spak Ulrik, « The common operational picture: A powerful enabler or a cause of severe misunderstanding? », 22nd ICCRTS, Track 4: Cognitive and Socio-technical Challenges, 8 janvier 2018. https://www.diva-portal.org/smash/get/diva2%3A1171677/FULLTEXT01.pdf?

de diffuser une image spatialement cohérente des informations obtenues sur le champ de bataille. C'est afin de répondre à cet enjeu qu'a été développé le programme GEODE 4D, qui vise à fournir aux armées françaises un système d'information regroupant l'ensemble des informations géospatiales disponibles (physiques, climatiques et hydrographiques) et leurs conséquences sur la conduite des opérations. La fusion d'un grand nombre de données de nature si différente place au centre des réflexions le processus de normalisation. Seule une normalisation efficace des formats de données et d'échange peut permettre le déploiement efficace des systèmes d'informations nécessaires à la bulle opérationnelle aéroterrestre. Si la production de normes visant à rendre disponibles des données géographiques sur les différents systèmes d'armes employés par les armées est déjà maîtrisée, répondre aux nouveaux besoins de la mise en réseau des différents capteurs est un défi auquel les armées n'ont pas encore su répondre totalement.

Dans ce domaine, la coopération internationale joue un rôle prépondérant. Tout d'abord, la mise en réseau des systèmes d'armes au sein des armées ne peut s'envisager de façon entièrement autonome. Le besoin de préparer les systèmes d'armes aux déploiements en coalition nécessite de pouvoir développer des normes fondées sur les normes internationales et sur celles produites en coopération avec nos alliés et partenaires. La construction d'une infrastructure de partage de données interalliées repose aujourd'hui sur le développement de projets internationaux de normalisation de données et capteurs multispectraux répondant aux exigences des armées. Ces projets s'appuient tous d'abord sur les normes internationales développées à l'ISO et à l'OGC concernant les capteurs et les données. Les passerelles tracées entre les différents comités techniques des instances internationales de normalisation dans différents domaines techniques permettent le développement de normes liant plusieurs domaines techniques. Ainsi, dans le cas des informations géographiques et des différents capteurs associés, le domaine des technologies spatiales et de la géomatique collabore régulièrement en matière de normalisation. Au sein de l'ISO/TC 211 le développement et l'actualisation de normes tels que l'« ISO/TS 19124 : Calibration et validation des données de télédétection et produits dérivés », l'« ISO/TS 19159 : Calibration et validation de capteurs de télédétection », ou l'« ISO/TS 19130 : Modèles de capteurs d'images de géopositionnement » reflètent ces développements conjoints.

D'autres projets internationaux se mettent également en place afin de développer des solutions en matière d'interopérabilité concernant les réseaux de données générés dans le cadre d'opérations militaires. Un de ces projets est porté par les États-Unis et porte le nom d'Integrated Sensor Architecture (ISA) que l'on pourrait traduire par « architecture de capteurs intégrés ». L'ISA est développée par l'Army Program Executive Officer for Intelligence, Electronic Warfare and Sensors (l'officier exécutif de programme de l'armée pour le renseignement, la guerre électronique et les

capteurs (PEO IEW&S))[713]. L'objectif principal de cette architecture est de permettre aux différents systèmes d'information de s'intégrer facilement dans un réseau préexistant et de partager dynamiquement des données et des informations afin de contribuer à la connaissance globale de la situation. En effet, les systèmes de capteurs habituels sont souvent développés « en silos » et nécessitent des protocoles de connexion spécifique pour paramétrer leur fonctionnement et accéder à leurs données. Chaque capteur nécessite une connexion point à point distincte, ainsi qu'un opérateur distinct, ce qui réduit la main-d'œuvre pour d'autres tâches. Ainsi, en 2012 l'armée américaine a relevé que, malgré l'utilisation très répandue de normes au sein de ses armes, son degré d'interopérabilité entre ses différentes unités restait très faible. Au moment du lancement du projet ISA l'armée américaine disposait de 116 systèmes d'information différents interagissant par le biais de 776 points de connexions propriétaires différents [714]. L'ensemble de ces connexions propriétaires sont déterminées avant le déploiement en opération. Ce manque de flexibilité une fois sur le champ de bataille entraîne un grand nombre de dysfonctionnements. Le problème est décuplé lorsqu'une zone comporte de nombreux systèmes d'informations et de capteurs, sans moyen de communiquer entre eux ou de contribuer à une connaissance partagée de la situation. Si un capteur est configuré pour fonctionner avec un autre système, la connexion doit être configurée avant le déploiement et doit être définie pour ces systèmes spécifiques, sans possibilité d'interopérer avec un futur système inconnu. Les anciens systèmes de capteurs reposent généralement sur des communications non sécurisées, ce qui les rend susceptibles d'être écoutés, manipulés (réponse à d'anciens messages, modification du contenu d'un message ou publication de fausses informations) et contrôlés par d'éventuels adversaires, ce qui accroît les risques en opération.

L'ISA doit permettre à l'armée américaine et à ses alliées de disposer d'une architecture permettant aux systèmes d'information de diffuser leurs informations afin de les mettre à la disposition des soldats et des plateformes de manière dynamique. Le tout, sans nécessiter de connaissance préalable de la part des opérateurs, et indépendamment du type ou de la propriété du système. L'ISA propose une solution interopérable conçue pour répondre aux besoins en matière de partage d'informations, notamment géographique, dans un environnement tactique. La capacité à maintenir le transfert d'information dans un environnement dégradé fait partie des priorités de l'ISA. Les exigences en matière de cybersécurité sont également au premier plan des défis à relever.

L'ISA est conçue comme une norme unique qui exprime de la même manière tout ce qui est lié aux capteurs. L'utilisation de l'ISA offre une large gamme d'applications. La spécification des données permet aux systèmes, même à ceux qui n'ont jamais été intégrés les uns aux autres auparavant,

[713] PEO IEW&S, « ISA Whitepaper », Document number 6.0, Revision Number 2, 31 octobre 2023, p. 3.
[714] PEO IEW&S, « Integrated Sensor Architecture », Integration Directorate, décembre 2023, p.2.

d'échanger des données dans un format commun. Le tout, sans nécessiter de modifications supplémentaires, de traducteurs ou d'autres adaptations du système une fois déployé en opération. Par conséquent, il suffit de configurer un système d'information pour qu'il communique avec un seul point de l'architecture, qui gère ensuite la création et la maintenance d'un réseau virtuel pour échanger des informations avec d'autres systèmes [715]. Les données étant définies selon un standard homogène, les capteurs peuvent définir ce qu'ils peuvent fournir, et les systèmes d'information connectés peuvent spécifier les informations dont ils ont besoin. Le réseau virtuel ISA échange des données concernant les besoins d'information des systèmes et les sources qui en disposent et relie de manière transparente les sources aux besoins afin de satisfaire de manière dynamique les demandes d'information des opérateurs. Les opérateurs, à leur tour, peuvent être alertés des éléments qui les intéressent. Les données diffusées en direct peuvent également être stockées et mises à disposition pour une requête ultérieure, en tant que données historiques. En utilisant les informations fournies par le réseau virtuel ISA, les éléments de commandement et de contrôle (C2) peuvent déterminer quelles informations sont disponibles et soutenir les demandes des opérateurs ainsi que l'affichage des informations personnalisées qui en résultent. Les opérateurs peuvent voir quels sont tous les capteurs et toutes les capacités, ce qui leur donne une image complète du champ de bataille et une meilleure connaissance de la situation. L'ISA fournit des services permettant aux opérateurs de spécifier les tâches à effectuer, telles que le changement de la direction de détection ou de l'emplacement à observer, le basculement des modes fonctionnels à utiliser (par exemple, visible ou infrarouge) et le déclenchement d'actions spécifiques (par exemple, l'obtention d'une distance à partir d'un télémètre laser). Les systèmes peuvent également choisir d'utiliser des services coopératifs pour déterminer les priorités des demandes et la propriété des capteurs. Par exemple, un opérateur peut réserver un ou plusieurs capteurs pour une période donnée, mais cette réservation peut être gérée et modifiée de manière dynamique si les circonstances changent.

Le développement de l'ISA a été initialement mené conjointement par l'armée américaine et l'armée britannique. Le Royaume-Uni dispose d'un nouveau programme appelé Zodiac[716] qui relie leurs différents capteurs entre eux en s'appuyant sur l'ISA comme standard commun. Afin de pouvoir déployer le système ISA au cours d'un engagement en coalition, l'armée américaine a décidé de s'appuyer sur le développement de normes ouvertes afin de faciliter l'adoption de cet architecture de système. Pour cela, les travaux conduits par l'OGC en matière de systèmes interconnectés sont étudiés de près. Ainsi, l'OGC a créé en 2001 un groupe de travail centré sur les systèmes connectés [717]. Celui-ci

---

715 PEO IEW&S, « ISA Introductory Guide », n° 6, 31 octobre 2023, p. 6.

716 Defence Procurement International, « ZODIAC : A central nervous system for the battlefield », 28 septembre 2021. https://www.defenceprocurementinternational.com/news/land/roke-to-develop-central-intelligence-system-for-land-istar

717 La liste des normes SWE est consultable sur le site de l'OGC. https://www.ogc.org/about-ogc/domains/swe/

se concentre sur la modernisation de la norme SensorML[718] et des normes connexes Sensor Web Enablement (SWE), tout en cherchant à anticiper les besoins concernant tous les types de systèmes connectés. Ce travail comprend la maintenance et la mise à jour de SensorML, y compris la finalisation des encodages JSON, l'adaptation d'approches modernes et RESTful aux normes SWE (pour la découverte, l'accès aux observations, les tâches et le traitement), et l'intégration de ces normes mises à jour avec d'autres API de l'OGC.

Une interface de programmation d'application (API) est un ensemble normalisé de fonctions et de procédures de programmation, qui exposent les capacités ou les données d'un système d'exploitation, d'une application ou d'un service à d'autres applications [719]. Le mot « application » désigne ici tout logiciel ayant une fonction distincte. L'interface dont il est question définit la manière dont le client et le serveur interagissent par le biais de requêtes et de réponses. La documentation de l'API contient des informations sur la manière dont les développeurs doivent structurer ces requêtes et ces réponses. Une API web est une API qui utilise un style architectural fondé sur les technologies du web [720]. Ainsi, si tous les services web sont des API, mais toutes les API ne sont pas des services web. L'API REST est un type particulier d'API Web qui respecte les principes de conception du style d'architecture REST, abréviation de « REpresentational State Transfer ». Ce style regroupe un ensemble de règles et de consignes pour la création d'API web[721]. Les API REST permettent d'accéder à des ressources géographiques (images satellite, cartes, objets vectoriels, etc.) via de simples requêtes HTTP structurées. Chaque ressource est identifiée par une URL unique, et les échanges se font généralement en JSON, GeoJSON ou XML, assurant ainsi une portabilité maximale entre différents environnements logiciels. Cette structuration repose sur un modèle client–serveur dans lequel l'API documente la forme des requêtes (GET, POST, PUT, DELETE) ainsi que les structures attendues en réponse. La grande popularité des API tient au fait qu'en publiant leurs API (sur le web), les organisations permettent aux développeurs de réutiliser et d'accéder aux fonctionnalités et aux données de leur API, tout en renforçant leur part de marché.

L'un des exemples les plus emblématiques de cette logique est fourni par le Géoportail de l'IGN, qui propose un ensemble complet de services API REST pour intégrer ses cartes topographiques, orthophotographies, modèles numériques de terrain ou limites administratives dans des

---

718 OGC, « OGC SensorML: Model and XML Encoding Standard », 10 août 2020. http://www.opengis.net/doc/IS/SensorML/2.1

719 ISO/IEC, « Technologies de l'information — Interopérabilité avec les technologies d'assistance, Partie 2 : Interface de programmation d'applications (API) d'accessibilité Windows », TR 13066-2 : 2016, édition 2, février 2016, p. 5.

720 OGC, « OGC API - Features - Part 1 : Core », 14 octobre 2019.

721 RedHat, « Une API REST, qu'est-ce que c'est ? », 2 février 2024. https://www.redhat.com/fr/topics/api/what-is-a-rest-api

outils tiers[722]. Ces API sont aujourd'hui utilisées tant par des collectivités territoriales pour l'aménagement du territoire que par des développeurs d'applications mobiles de randonnée ou de visualisation urbaine. Elles sont accessibles via des appels directs à des URL documentées et renvoient des flux de données interopérables conformes aux spécifications de L'Open Geospatial Consortium (OGC) Dans le secteur privé, des plateformes globales comme Google Maps Platform, OpenStreetMap ou Amazon Location Services ont également recours à des API REST. Par exemple, l'API Routes (anciennement Direction) de Google permet de générer des itinéraires en fonction de coordonnées géographiques transmises par URL[723], tandis que Overpass API d'OpenStreetMap permet d'interroger la base cartographique communautaire en langage QL pour extraire des couches spécifiques (routes, hôpitaux, lignes électriques, etc.)[724]. Ces interfaces, conçues selon les standards REST, permettent aux utilisateurs de créer des visualisations dynamiques, des modèles prédictifs spatiaux, ou encore des outils de monitoring territorial. Dans le domaine militaire et de la géographie opérationnelle, les API REST revêtent un caractère stratégique. Le projet américain ISA (Integrated Sensor Architecture) illustre la manière dont une architecture normalisée d'API REST peut permettre de relier entre eux des capteurs hétérogènes, comme des drones, des radars, des satellites, ou encore des véhicules blindés. Chaque système est exposé comme une ressource accessible via API, permettant une agrégation et une exploitation centralisée des données en temps réel[725]. Le champ de bataille devient alors une structure distribuée d'objets géolocalisés interopérables, où la position, le statut et les données des équipements sont consultables via des services RESTful. L'usage des API REST est également intégré dans les systèmes européens, comme la plateforme Copernicus Open Access Hub, qui met à disposition les images satellites Sentinel via des API REST conformes à la norme OGC API Features (anciennement WFS3)[726]. Ces données sont utilisées par les autorités nationales pour le suivi des catastrophes, la surveillance environnementale ou la cartographie d'urgence. Dans ces différents cas, l'enjeu dépasse la seule commodité technique, il s'agit de garantir un accès normé, sécurisé et contrôlable aux flux géospatiaux. L'usage d'API REST permet d'instaurer une couche d'abstraction interopérable entre des bases de données dispersées, tout en favorisant une gouvernance distribuée de la donnée géographique, notamment dans les contextes multiacteurs (collectivités, entreprises, institutions militaires). Enfin, la normalisation croissante des API REST s'inscrit dans une dynamique plus large, celle de la gouvernance algorithmique des territoires. En rendant l'espace requêtable à distance via des interfaces

[722] La liste complète des fonctionnalités offertes par les API de la Géoplateforme sont disponibles sur le site géoservice de l'IGN. https://geoservices.ign.fr/documentation/services/services-geoplateforme. Consulté le 9 juillet 2025.

[723] La documentation de l'API Routes de Google est disponible sur le site Google Maps Plateforme. https://developers.google.com/maps/documentation/routes?hl=fr. Consulté le 9 juillet 2025.

[724] https://wiki.openstreetmap.org/wiki/Overpass_API. Consulté le 9 juillet 2025.

[725] PEO IEW&S Integration Directorate, *Integrated Sensor Architecture*, PEO IEW&S Integration Directorate, décembre 2023. https://peoiews.army.mil/wp-content/uploads/2023/12/ISA-Panel-TEM-11.pdf. Consulté le 12 juillet 2025.

[726] https://www.copernicus.eu/en/access-data/conventional-data-access-hubs. Consulté le 12 juillet 2025.

standardisées, les API REST modifient profondément la façon dont les acteurs politiques, économiques ou militaires interagissent avec l'espace géographique, et comment ils le modèlent, le contrôlent ou le contestent. Ces technologies participent ainsi à la fabrique algorithmique des territoires, où l'interface devient une infrastructure d'accès à la réalité spatiale. Les normes API, bien que relativement récentes, sont particulièrement utiles pour les applications modernes en ligne et mobiles en raison de leur adaptabilité et de leur dynamisme accrus. Ces normes sont centrées sur les ressources et donnent la priorité à la mise à disposition de données géographiques et de fonctionnalités en tant que ressources distinctes auxquelles on peut accéder par le biais d'URL. Par conséquent, elles deviennent non seulement l'option préférée des développeurs, mais les entreprises les jugent également de plus en plus nécessaires pour adopter de nouvelles technologies et améliorer leur capacité d'accès et d'analyse des données et des services géographiques.

Ainsi, avec l'émergence de l'internet des objets (IoT) et la multiplication des capteurs de toutes natures, ainsi que leur miniaturisation, l'OGC a décidé de créer son propre groupe de travail dédié au développement d'API dédié à faciliter l'interconnexion des appareils, des données et des applications de l'internet des objets sur le Web. Il s'agit du SensorThingsAPI[727]. Parallèlement, la miniaturisation et la multiplication des capteurs, ainsi que les innovations en matière de traitement avancé, ont entraîné une explosion de capteurs interconnectés dans des secteurs tels que les bâtiments intelligents, les villes intelligentes, ou encore la robotique. Un nombre considérable de satellites de télédétection et de communication ont été mis en orbite, et des drones de toutes sortes sont devenus des plateformes dynamiques permettant non seulement de détecter, mais aussi d'entreprendre toutes sortes de tâches. Rapidement, la question de l'interconnexion de l'ensemble de ces capteurs s'est posée. L'internet des objets est progressivement devenu l'internet de tout. Cette situation a mené à la création d'un ensemble cohérent de définitions sémantiques normalisé pour la description de ces systèmes. L'OGC et le W3C se sont associés pour développer le Semantic Sensor Network Ontology (l'ontologie sémantique des réseaux de capteurs)[728], en s'inspirant largement des travaux antérieurs sur SensorML et l'Observation, Measurements, and Samples (Observations, mesures et échantillonnages ou OMS)[729]. Ces définitions et d'autres complémentaires ont jeté les bases d'une intégration cohérente des systèmes connectés d'une manière qui permette d'en saisir et d'en transmettre le sens. C'est dans ce contexte qu'a été créé un nouveau projet de norme pour une IPA OGC dédié aux systèmes connectés, « OGC API - Connected Systems Standard »[730] a été créé en 2022. Cette norme s'appuiera sur des formats web reconnus tels que

[727] Page internet de l'OGC dédié au SensorThings API : https://ogcapi.ogc.org/sensorthings/

[728] Page internet du W3C dédié au Semantic Sensor Network Ontology. https://www.w3.org/TR/vocab-ssn/

[729] https://www.ogc.org/standard/om/

[730] La spécification OGC API - Connected Systems relie tous les systèmes sur ou autour de la Terre dans un cadre 4D commun à des fins de découverte, d'accès, de traitement, de raisonnement, de visualisation et d'attribution de tâches à toutes sortes de systèmes (p. ex, capteurs, objets, robots, drones, satellites, et toutes sortes de plateformes dans l'espace,

GeoJSON, ainsi que sur les modèles d'information existants de l'OGC, notamment SensorML, OMS, SWE et Semantic Sensor Network Ontology. Le but de cette API est de faire le lien entre les données statiques, notamment géographiques, et les données dynamiques elles-mêmes tirées des observations des données statiques et notamment des actions qui modifient ces propriétés. Ainsi, l'API sera une extension de l'API « OGC - Features » et, en plus de fournir son propre mécanisme d'extraction de données statiques et dynamiques, l'API permettra d'établir des liens avec d'autres API de l'écosystème OGC, telles que 3D GeoVolumes, 3D Tiles, Coverages, EDR, SensorThings, Moving Features, Processes, etc.

De même, un groupe de travail au sein du DGIWG a été créé en juillet 2023 afin de développer un profil des normes OGC et ISO dans ce domaine, adapté aux besoins des acteurs de la défense. Au sein du DGIWG ce groupe de travail mêle des membres de l'U.S. Sensor Integration Framework Working Group (SIFWG) et des membres du P5 (services web) ainsi que du P2 (Imagerie et données maillées). Le SIFWG est un groupe de travail chargé de créer un cadre d'intégration des capteurs (SIF) pour le partage des capteurs dans les environnements tactiques, conformément aux politiques du ministère américain de la Défense et sur la base de normes ouvertes. Le travail du SIFWG se concentre sur le partage des métadonnées des capteurs GEOINT et MASINT par le biais de normes internationalement reconnues et de façon à répondre aux besoins de l'armée américaine et de ses alliées. Ce groupe de travail conjoint doit permettre d'identifier les normes qui comblent les lacunes et les limites liées à l'intégration des données et des procédures des capteurs pour le renseignement, la surveillance et la reconnaissance (RSR) dans les domaines suivants : Découverte, accessibilité, compréhension, fiabilité, sécurité et interopérabilité. Le but étant de produire un profil DGIWG des normes existantes qui permettent le partage des informations et des observations d'un ensemble de capteurs, entre des systèmes logiciels accrédités au sein d'un environnement informatique partagé dans le cadre d'un engagement en coalition. Produire un profil DGIWG de la norme OGC en matière d'intégration de capteurs pourrait être une solution pour établir une première norme partagée par les pays membres du DGIWG. Il est à noter qu'au sein de l'OTAN, il n'existe pour le moment qu'un seul standard, le STANAG 4789, définissant les modalités de partage de données entre plusieurs réseaux de capteurs au sein de l'Alliance atlantique. Le STANAG 4789 est encore aujourd'hui à l'état de projet (draft), bien que des tests relatifs à son application en engagement ont déjà été réalisés depuis 2021[731].

---

l'air, la terre, la mer et le cyberespace), en fournissant un pont entre leurs données dynamiques (par exemple, les observations de ces propriétés d'entités et les commandes qui modifient ces propriétés d'entités) et les représentations plus statiques de celles-ci en tant qu'entités dans les applications géographiques/géospatiales traditionnelles. Source : OGC, « Draft OGC API - Connected Systems – Part 1 : Feature Resources », 1er février 2024.

731 NATO STO, « Interoperability & Networking of Disparate Sensors and Platforms for Tactical ISR Applications conducts successful live experiment », NATO STO News Archive, 3 janvier 2022. https://www.sto.nato.int/_layouts/mobile/dispform.aspx

Aujourd'hui, les forces de l'OTAN ne peuvent pas tirer efficacement parti des moyens mobiles et fixes de renseignement, de surveillance et de reconnaissance (ISR) (capteurs, caméras, capteurs au sol sans surveillance, etc.) des partenaires de la coalition pendant les opérations terrestres de l'Alliance atlantique. Les partenaires de la coalition doivent fournir tous les moyens ISR dont ils ont respectivement besoin, ce qui entraîne une augmentation significative des coûts de logistique, de maintien en condition opérationnelle et de personnel. L'objectif de ce test était d'aider à établir un processus décisionnel visant à augmenter la disponibilité des informations provenant des systèmes ISR des membres de la coalition. Jusqu'à ce qu'une solution normalisée soit trouvée, les forces de la coalition continueront à ne pas pouvoir partager efficacement les données des leurs divers capteurs, ce qui se traduira par une connaissance incomplète de la situation.

Avec le tournant effectué par l'OGC vers OpenAPI et le développement de normes API visant à remplacer les anciennes normes de services web, telles que OGC Sensor Web Enablement (SWE), le DGIWG et le MASINT Working Group de l'armée américaine se tournent également vers ces nouvelles normes de l'OGC pour bâtir la nouvelle architecture ISR de l'OTAN. Les services Web traditionnels de l'OGC (OWS) sont un ensemble de normes développées par l'Open Geospatial Consortium (OGC) pour soutenir le partage et le traitement interopérables des données géospatiales sur le Web. Ils sont généralement décrits comme étant centrés sur les services. Cela signifie qu'elles suivent une architecture orientée services (Service Oriented Architecture : SOA) et sont conçues pour permettre une interaction interopérable de machine à machine sur un réseau et sont spécifiquement axées sur le partage/la fourniture de données ou de fonctionnalités géospatiales. Les SOA utilisent un processus Publish-Find-Interact (publier, trouver, interagir). Les principales normes OWS comprennent le service de carte Web (WMS), le service d'entités Web (WFS), la couverture Web (WCS), etc. Les normes API de l'OGC sont des protocoles de nouvelle génération conçus pour moderniser et simplifier l'accès et l'intégration des données géospatiales. Elles sont généralement décrites comme des services orientés ressources, au contraire des normes des architectures SOA. Cela signifie qu'elles se concentrent sur l'a mise à disposition des données et des fonctionnalités géospatiales en tant que ressources, représentées par des URL uniques.

Il y a plusieurs différences fondamentales entre les anciens services web OWS de l'OGC et les nouvelles API, qui contribuent à l'adoption progressive des normes API aux dépens d'OWS. Tout d'abord, les normes OWS reposent sur le langage XML, ce qui nécessite une analyse et un traitement plus complexes, alors que les normes fondées sur les API reposent sur les principes RESTful avec JSON, ce qui offre une approche plus légère et plus accessible. Les API OGC sont conçues pour être faciles à utiliser et permettre un développement et une intégration plus rapides avec les technologies web modernes. Au contraire, les normes OWS nécessitent des connaissances et des outils plus

spécialisés pour être mis en œuvre et utilisés efficacement. Les services basés sur les API sont conçus pour être plus adaptables et plus faciles à développer que les services OWS, plus rigides et plus complexes. Les services basés sur les API permettent de décloisonner les architectures étroitement intégrées et de favoriser la flexibilité. Enfin, en termes de performance, ces services sont généralement plus rapides et plus efficaces, bénéficiant de la légèreté de REST et JSON, que les services OWS fondés sur XML. Alors que les OWS traditionnels ont jeté les bases de l'échange de données géospatiales interopérables, les normes API de l'OGC représentent une évolution significative vers des services géospatiaux sur le web plus efficace, plus accessible et plus moderne. Avec la popularité grandissante des API OGC, la communauté de la défense se doit de s'intéresser de près à ces développements afin de faciliter l'interopérabilité des systèmes civilo-militaires et internationaux. C'est dans cette optique que le DGIWG a développé sa note d'intention concernant l'emploi potentiel des API OGC pour répondre aux besoins des armées.

Plusieurs normes de l'OGC intéressent le MASINT Working Group à commencer par l'« OGC Sensor Things API » et l'« OGC API connected systems ». La production d'un profilé des normes OGC validé par le DGIWG pourrait permettre le développement d'un STANAG OTAN fondé sur un guide d'implémentation des fonctionnalités contenues dans les normes OGC API adaptés aux besoins de la communauté de la défense. Aujourd'hui, le STANAG 6523 portant sur les services web géospatiaux fonctionne déjà sur ce modèle et s'appuie sur les profilés des standards OGC développés par le DGIWG[732]. L'existence d'exercices tels que CIWIX où les services Web de l'OTAN sont testés permet de faire remonter de nouveaux besoins en matière de partage d'informations géographiques et d'architecture multicapteurs. Les exercices CIWIX permettent aussi d'entraîner les opérateurs à maîtriser les nouvelles normes et les systèmes qui s'appuient dessus. Concevoir et appliquer des normes dans des coalitions militaires telles que l'OTAN nécessite de suivre attentivement à la fois les avancées technologiques et les besoins exprimés par les opérateurs. Rédiger un document normatif n'est qu'une première étape, seuls l'entraînement et le suivi post-adoption du standard peuvent assurer sa maîtrise par les acteurs concernés et in-fine son efficacité.

Dans le cadre du développement de ce nouveau standard, les défis à relever sont nombreux et tiennent en particulier à l'aspect novateur de ce projet, qui mêle un grand nombre de normes différentes, qui sont pour beaucoup toujours à l'état de projet ou en cours de développement. Cet aspect avant-gardiste tranche avec la réalité des membres de la coalition qui n'ont pas encore pleinement envisagé l'exploitation qu'ils pourraient faire des API de l'OGC en matière de partage d'informations. En effet, les systèmes d'information exploités par les forces armées reposent avant tout sur les normes

[732] NATO, « AgeoP-26 DEFENCE GEOSPATIAL WEB SERVICES », Edition A, Version 1, NATO STANDARDIZATION OFFICE (NSO), mars 2020.

OWS telles que WMS, WMTS, et non sur les API qui n'ont pas encore été adoptés massivement. De plus, certaines normes OGC API sont encore en cours de développement, comme OGC API Connected Systems. La question de la cybersécurité occupe également une place centrale. Les standards OGC étant construits dans l'optique de s'adapter au plus d'usages potentiels possible sont rarement construits avec un fort accent mis sur les questions de sécurité. De fait, renforcer les règles de sécurité d'un standard tend à restreindre ses modalités d'adoption. La question de l'implémentation de mesures de sécurité au sein des normes pose également le problème de leur actualisation. Inclure ces mesures dans la norme permet de s'assurer du respect de mesures fondamentales de cybersécurité par l'ensemble des utilisateurs, sans avoir à se reposer sur le travail ultérieur d'experts en sécurité des réseaux. Cependant, si les mesures de cybersécurité deviennent obsolètes, alors même que le reste des règles d'implémentations du standard ne changent pas, cela peut poser des difficultés aux utilisateurs. Ces derniers sont souvent réticents à voir évoluer les standards trop régulièrement, en particulier dans le milieu de la défense où l'adoption de nouveaux standards peut prendre beaucoup de temps. Le choix de la NGA et du ministère de la défense américain de s'appuyer sur les normes OGC API démontre une volonté de se maintenir à la pointe des avancées technologiques en matière de diffusion des informations géographiques. Cependant, alors que le développement de certaines de ces normes n'est pas achevé, les modalités d'exploitation exacte des API de l'OGC au sein des armées reste encore à définir.

Aujourd'hui, le projet conjoint du DGIWG et de l'armée américaine laisse tout de même augurer d'une adoption prochaine des normes OGC en matière d'API. Ainsi, s'il est vrai que la spécification de la norme OGC API Connected Systems, visant à moderniser et à remplacer l'ancien cadre API Sensor Web Enablement (SWE), est actuellement à l'état de projet, celle-ci est fondée sur une extension d'une norme déjà approuvée par l'OGC : « OGC API – Features ». De plus, la constitution de ce groupe de travail devrait permettre aux participants de collaborer avec l'OGC et d'influencer sur le développement de prochaines normes API. Ce projet est également aligné sur les orientations définies dans la stratégie de l'OTAN sur « Les technologies émergentes et de rupture » pour la défense, notamment concernant les réseaux de communication de nouvelle génération [733]. Dans le même temps, le DGIWG a prévu de publier une note d'intention décrivant les avantages potentiels pour les armées à adopter l'usage des API pour leurs systèmes d'information [734]. Ce projet est également aligné avec la stratégie du ministère américain de la Défense sur les données [735]. Il atténue

[733] OTAN, « Technologies émergentes et technologies de rupture », 31 mai 2024. https://www.nato.int/cps/en/natohq/topics_184303.htm?selectedLocale=fr

[734] DGIWG, « DGIWG API Whitepaper », Édition: x.0.3, 5 avril 2024.

[735] Department of Defense, « Executive Summary: DoD Data Strategy : Unleashing Data to Advance the National Defense Strategy », Office of Prepublication and Security Review, 30 septembre 2020, p. 7.

également le risque de voir les programmes de l'OTAN et des États-Unis progresser sans la mise en œuvre de normes appropriées et approuver conjointement, tout en maintenant ces programmes à jour du point de vue des évolutions technologiques en matière de communication et d'échange de données. Il s'agit également d'une opportunité de s'assurer que la norme API de l'OGC soit conçue en prenant en compte les besoins de la communauté de la défense. Il reste encore à harmoniser non seulement les besoins exprimés par les différents acteurs, mais également les calendriers en matière de programme de normalisation, entre les impératifs de l'OTAN, du DGIWG et des programmes de développement militaires américains. L'ensemble de ces organisations ne suivent pas nécessairement des calendriers de développement similaires, et la gestation d'un projet de norme peut varier très largement d'une organisation à l'autre.

Conclusion du Chapitre V

En conclusion, ce chapitre a permis de mettre en évidence la centralité des normes dans les processus de structuration des infrastructures géonumériques militaires, à travers l'exemple de l'Integrated Sensor Architecture (ISA). En adoptant une lecture géographique de cette architecture technique, il devient clair que les normes ne peuvent être réduites à de simples instruments de coordination technologique. En effet, elles participent pleinement à la construction sociale et opérationnelle de l'espace militaire contemporain. Dans une perspective proprement géographique, les normes définissant l'interopérabilité des capteurs, des systèmes de commandement et des flux d'information agissent comme des vecteurs de spatialisation. Elles traduisent la volonté institutionnelle et stratégique de représenter, de maîtriser et d'agir sur le territoire via des données géoréférencées, transmises et synchronisées à différentes échelles. L'espace militaire tel qu'il se dessine dans les architectures comme ISA n'est plus uniquement un substrat physique, mais un espace de flux, composé de réseaux capteurs, de nœuds décisionnels, et de topologies informationnelles qui structurent les opérations militaires. Autrement dit, la norme devient ici un dispositif de mise en géographie du champ de bataille. Ce changement d'échelle et de registre impose une relecture des concepts classiques de la géographie militaire. La territorialité n'est plus seulement fondée sur la possession ou l'occupation de l'espace physique, mais sur la capacité à produire et exploiter des données spatiales en temps réel. À travers les normes, les armées structurent leur rapport à l'espace en en délimitant les représentations, les hiérarchies, les zones d'intérêt et les corridors de communication. Le territoire devient alors un objet codé, produit et agi selon des logiques informationnelles normalisées. Méthodologiquement, cette évolution appelle à un renouvellement des outils d'analyse géographique. Les notions de réseau, de dispositif technique, de milieu numérique et de territoire algorithmique deviennent incontournables pour comprendre l'emprise des normes sur les formes contemporaines de spatialisations militaires. Les normes, loin d'être neutres, orientent les représentations de l'espace, déterminent ce qui est mesurable, observable ou actionnable, et participent donc à la construction d'un territoire opérationnel géonumérique, fondé sur des logiques de visualisation, d'interopérabilité et de contrôle. Dans cette optique, le géographe militaire se voit confier un rôle crucial, il lui revient d'analyser comment ces infrastructures numériques produisent des effets d'espace, comment elles redéfinissent les échelles de l'action militaire, du soldat connecté au théâtre d'opérations transnational, et comment elles modèlent la géographie des conflits futurs. L'étude des normes ne peut se faire sans une attention fine aux conditions géographiques de leur production, de leur circulation et de leur mise en œuvre. Qu'il s'agisse des lieux de développement (centres de R&D, laboratoires militaires), des logiques

d'appropriation (alliances, coalitions), et des tensions géopolitiques qu'elles cristallisent (souveraineté, dépendance, interopérabilité). Ce chapitre montre ainsi que les normes technologiques ne sont pas extérieures à l'espace géographique, mais en sont des productrices actives, qui contribuent à reconfigurer la manière dont les armées conçoivent, organisent et opèrent sur le territoire. Elles constituent, à ce titre, un objet d'étude central pour une géographie militaire critique et informée des enjeux numériques.

De fait, les plateformes d'information géographiques sont aujourd'hui d'une importance capitale pour la société civile, comme la communauté militaire. Principale porte d'entrée pour l'accès et la diffusion des données géographiques, ces dernières sont pourtant vulnérables à de potentielles attaques cyber. Le maintien en fonctionnement de ces infrastructures est aujourd'hui d'une grande importance, en termes de souveraineté, de responsabilité économique, et de justice territoriale. Le maintien de la mise à disposition des données géographiques doit permettre aux citoyens d'exercer leur droit à connaître leur territoire et à disposer de données fiables et garantie par la puissance étatique sur celui-ci. Avec la recrudescence des attaques cyber, corrélé avec la montée des tensions internationales, la défense des systèmes d'information géographiques doit être à la hauteur du risque qui pèse sur elles. Les systèmes de communication militaires, pour qui la localisation et le géopositionnement sont des données essentielles à la manœuvre, doivent également faire face à un risque accru en cas de dysfonctionnement de ces systèmes au cours d'un affrontement. Face à cela, la normalisation des données tient un rôle essentiel, en facilitant non seulement la diffusion des données, mais également en renforçant la résilience des systèmes d'information par le développement de normes de sécurité à même de diffuser au sein des communautés d'utilisateurs et de développeurs, des bonnes pratiques essentielles en matière de protection de ces données. Si la communauté militaire cherche activement à développer des systèmes d'information robustes capables de fonctionner dans des conditions dégradées ou sous la menace d'interférences, ces considérations ne sont pas encore pleinement assimilées au sein de la communauté civile. Cette dernière peine toujours, en particulier au sein des échelons infranationaux, à prendre la juste mesure du risque cyber, mais nos territoires, plus encore que nos armées, sont le cœur de cible de potentiels pirates informatiques qui, s'ils sont souvent moins bien équipés que des armées modernes contre lesquelles nos forces armées se préparent, trouvent tout de même dans les régions et les collectivités locales des cibles d'opportunités qu'ils n'hésitent pas à frapper. Protéger nos territoires et leurs systèmes d'informations géographiques reste aujourd'hui un défi important, auquel il est nécessaire de faire face afin de garantir la préservation, la diffusion et l'exploitation des données géographiques.

Chapitre VI- Les territoires au défi de la protection des données géographiques numériques

Le chapitre précédent a mis en lumière les vulnérabilités des infrastructures de données géographiques à l'échelle nationale et internationale, ainsi que les dispositifs institutionnels et normatifs déployés pour y répondre. L'analyse a révélé que la protection de ces infrastructures critiques mobilise des acteurs de premier plan, (l'IGN, le CNIG, l'ANSSI, les instances de l'OTAN) et s'inscrit dans des logiques de souveraineté numérique qui dépassent largement le seul cadre technique. Toutefois, cette focale sur les échelons supérieurs de la gouvernance ne saurait épuiser la complexité des enjeux territoriaux. Car les données géographiques ne sont pas seulement produites, stockées et diffusées par des plateformes nationales, elles irriguent l'ensemble du tissu territorial, des métropoles aux communes rurales, des conseils régionaux aux syndicats intercommunaux. C'est à cette échelle infranationale, souvent négligée dans les analyses stratégiques, que se jouent pourtant des défis décisifs en matière de protection des données géographiques numériques.

Le présent chapitre opère ainsi un changement d'échelle, en portant le regard sur les territoires et leurs acteurs. Les collectivités territoriales sont aujourd'hui des productrices majeures de données géographiques, qu'il s'agisse des plans cadastraux numérisés, des bases adresses locales, des données d'occupation du sol ou des référentiels d'urbanisme. Leur contribution à l'écosystème national de la donnée géographique est considérable, bien que souvent invisibilisée. De plus, il est nécessaire d’intégrer dans cette analyse les rapports de pouvoir, les inégalités de ressources et les conflits de légitimité qui structurent les relations entre les différents échelons territoriaux, afin de mieux saisir la véritable géopolitique locale et les rivalités qui se nouent autour du contrôle de l’information géographique[736].

Le contexte institutionnel français confère à cette problématique une acuité particulière. La loi NOTRe de 2015[737] a renforcé le rôle des Régions dans la coordination de l'information géographique, tout en maintenant les prérogatives de l'État en matière de référentiels nationaux. Cependant, cette architecture à plusieurs niveaux engendre des tensions récurrentes. Les collectivités se voient confier des responsabilités croissantes en matière de production et de diffusion de données, sans toujours

[736] Sur la notion de « fracture numérique territoriale », voir Dupuy Gabriel, La fracture numérique, Ellipses, 2007 ; et Eveno Emmanuel, « La géographie de la société de l'information : entre abîmes et sommets », Netcom, vol. 18, n° 1-2, 2004, p. 11-87.

[737] Loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République (loi NOTRe), JORF n° 0182 du 8 août 2015.

disposer des moyens humains, techniques et financiers nécessaires à leur mise en œuvre[738]. Le paradoxe est important, alors même que l'État attend davantage d'autonomie et de participation des territoires à la production de données géographiques, de nombreuses collectivités demeurent confrontées à des contraintes budgétaires et à une pénurie de compétences spécialisées, notamment en matière de cybersécurité. Cette asymétrie creuse une fracture numérique territoriale qui ne recoupe qu'imparfaitement les clivages traditionnels entre espaces urbains et ruraux, entre régions riches et régions périphériques.

La question de la cybersécurité constitue le fil rouge de ce chapitre. Les collectivités territoriales sont devenues des cibles privilégiées des cyberattaques, comme en témoigne le recensement de l'ANSSI qui dénombre 218 incidents touchant ce périmètre en 2024[739]. Les conséquences de ces attaques (interruption des services publics, vol de données sensibles, paralysie des systèmes d'information géographique), affectent directement la capacité des territoires à exercer leurs compétences et à conduire leurs politiques d'aménagement. Or, la protection des données géographiques à l'échelle locale ne peut être pensée indépendamment des rapports de force qui structurent les relations entre collectivités et État[740]. L'accès aux données, leur gouvernance, les choix technologiques imposés ou négociés, ou encore les standards à respecter, sont autant de dimensions où se manifestent des logiques de centralisation et de résistance, de coopération et de conflit, qui façonnent la géographie effective de la protection des données géographiques.

Ce chapitre s'organisera en trois temps. La première partie examinera les enjeux de la protection des données géographiques à l'échelle infranationale, en analysant le rôle des départements et des communes comme producteurs de données, leur vulnérabilité face aux cybermenaces, et les conséquences des attaques sur le fonctionnement des services territoriaux. La deuxième partie s'attachera à l'importance des standards de données comme instruments de coordination et de sécurisation, en étudiant les projets nationaux de normalisation, les difficultés de gouvernance entre l'État et les collectivités, et les obstacles à l'accès aux données. Enfin, la troisième partie proposera une étude de cas approfondie du programme de Jumeau numérique de la France et des Territoires (JNFT)[741], qui cristallise les tensions entre innovations technologiques, exigences d'interopérabilité et impératifs de cybersécurité. Ce projet, par son ambition et sa complexité, offre un terrain d'observation privilégié

---

738 Sur les asymétries de ressources entre collectivités en matière numérique, voir le rapport de la Cour des comptes, Les collectivités territoriales et le numérique : des ambitions à la transformation, janvier 2024.

739 ANSSI, Panorama de la cybermenace 2024, 2025. Le rapport recense 218 incidents cyber touchant les collectivités territoriales en 2024, soit une moyenne de 18 incidents par mois.

740 Sur la géopolitique locale et les conflits d'aménagement, voir Subra Philippe, Géopolitique locale. Territoires, acteurs, conflits, Armand Colin, 2016.

741 Le programme du Jumeau numérique de la France et des Territoires (JNFT) a été lancé par l'IGN en 2023, avec l'ambition de constituer une réplique virtuelle du territoire national intégrant données géographiques, environnementales et urbaines

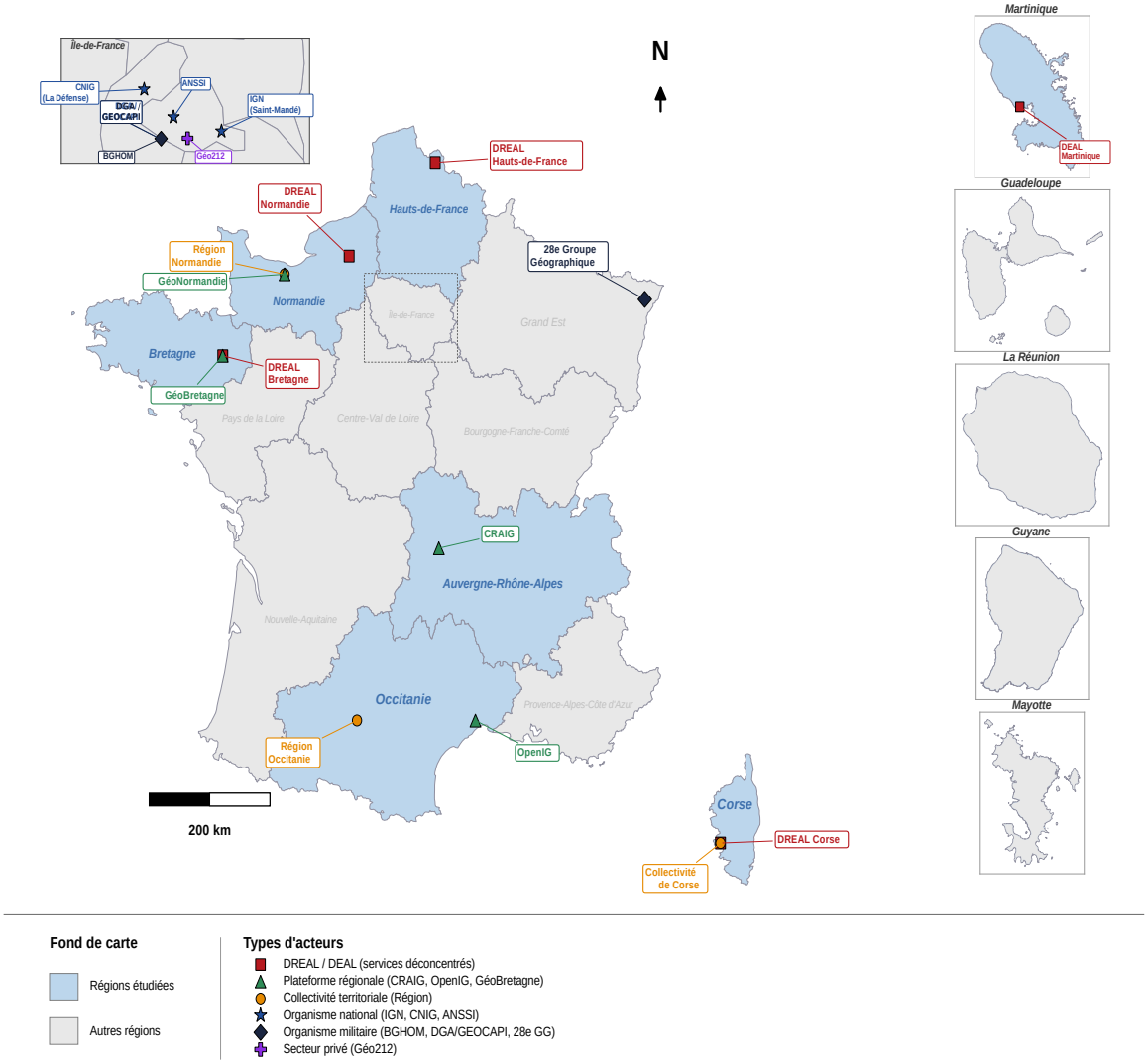
des défis auxquels sont confrontés les territoires dans la protection de leurs données géographiques numériques.

L'enjeu de ce chapitre est ainsi double. Sur le plan empirique, il s'agit de documenter les réalités concrètes auxquelles sont confrontées les collectivités territoriales : manque de moyens, dépendance technique, difficultés d'accès aux données, vulnérabilités face aux cyberattaques. Sur le plan analytique, il s'agit de montrer que la protection des données géographiques ne peut être réduite à une question technique ou juridique : elle constitue un enjeu géopolitique à part entière, qui engage les rapports de pouvoir entre territoires, entre niveaux de gouvernement, et entre acteurs publics et privés. Le cadre réglementaire européen, avec l'entrée en vigueur du Data Governance Act[742] et du Data Act[743], ajoute une strate supplémentaire de complexité, en imposant de nouvelles obligations en matière de gouvernance et de partage des données auxquelles les collectivités doivent s'adapter. En portant l'attention sur les territoires, ce chapitre entend ainsi contribuer à une géographie politique de la donnée géographique, attentive aux échelles, aux acteurs et aux conflits qui façonnent la production, la circulation et la protection de l'information spatiale à l'ère numérique.

[742] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (Data Governance Act)

[743] Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (Data Act).

Carte 5 : Acteurs de l'information géographique dans les territoires étudiés



Source : Enquêtes de terrain de l'auteur (2022 – 2024)

1. Protéger les données géographiques numériques à l'échelle infranationale

Les données de toute nature constituent aujourd'hui des denrées précieuses produits et consommés à toutes les échelles du territoire par de nombreux acteurs. Aux échelles infranationales (régionale, départementales et communales), la maîtrise de ces données constitue un enjeu de premier plan pour le développement des territoires. Les données géographiques ne font pas exception à cette règle, bien au contraire, puisqu'elles constituent des données essentielles pour l'observation des évolutions de ces mêmes territoires. Si, encore aujourd'hui, seuls 16 % des collectivités respectent l'obligation d'ouverture des données [744], il n'en reste pas moins que l'intérêt pour la réutilisation des données géographiques se développe sur l'ensemble du territoire. Comme souligné au chapitre précédent, le développement et l'entretien des plateformes d'information géographique soulignent une prise de conscience de plus en plus affirmée de l'importance de ces données. Cependant cette volonté de développer la production et la maîtrise de ces données, ainsi que leur protection est parfois contrariée, notamment pour des raisons de manque de moyens ou de personnels. En particulier dans le cas de la protection des données, où des compétences de pointe sont nécessaires, ce qui rend le recrutement de tels agents souvent difficile dans certains territoires. À ces problématiques s'ajoutent celles de l'acculturation aux données géographiques, qui rend parfois leur réutilisation ardue. Il faut également prendre en compte la question des relations entre les collectivités et l'État. Ces dernières butent parfois sur certains points, notamment la grande verticalité de ces relations, soulevant du même coup des problèmes de gouvernance concernant la gestion des données géographiques. La relation entre les directives données en matière de protection des données, notamment concernant les attaques cyber, et les conditions actuelles de leur mise en pratique sont également les témoins de dysfonctionnement dans les relations entre les collectivités et l'État. Concernant la protection des données, l'évolution du cadre juridique national et européen constitue également un défi pour les collectivités en charge de mettre en place les nouvelles directives, telles que le Data Governance Act[745] (sur la gouvernance des données) ou le Data Act[746] (sur les données). Il apparaît aujourd'hui que la normalisation des données en facilitant le passage à l'échelle les échanges et la mutualisation des données, en facilitant la création d'espace commun de données, peut aider à résoudre les problèmes en matière de gestion et de

[744] Hennion Christine, Altounian Magali et Monthubert Bertrand, « Rapport de la Mission Data et Territoires », Ministère de la Transformation et de la Fonction Publique, septembre 2023, p. 21.

[745] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données).

[746] Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données).

protection des données géographiques par les collectivités. Le développement collaboratif des normes doit être facilité et étendu à un maximum d'acteurs possibles afin de maximiser les retombées positives une fois qu'ils sont acceptés. Comme le recommande la mission Data et territoires, il convient aussi d'industrialiser la fabrication des standards et d'en faciliter la diffusion[747]. Le développement d'espace commun de données, fondées sur des standards largement acceptés, doit permettre la diffusion et leur alimentation par le plus grand nombre. Ils constituent des outils essentiels aux services des territoires et leur alimentation suppose, selon la même mission, la mobilisation des collectivités territoriales comme des acteurs privés[748]. De plus, la normalisation des mesures de cybersécurité au sein des infrastructures de données géographiques devrait permettre à terme une plus large diffusion de ces dernières au sein des collectivités, à la condition que des solutions soient trouvées aux problèmes des moyens matériels et humains actuellement rencontrés par nombre d'entre elles. En effet, concernant les moyens humains, un manque certain de spécialistes en matière de cybersécurité se fait sentir dans de nombreuses régions. De plus, les formations aujourd'hui proposées en matière de cybersécurité et de gestion de données ne sont pas toujours suffisamment nombreuses ou adaptées aux enjeux contemporains.

1.1 Les départements et les communes : acteurs importants, mais fragiles de la production de données géographiques

Les collectivités territoriales ne sont pas uniquement des utilisatrices de données produites à l'échelle nationale, bien que ce rôle soit souvent mis en avant. En réalité, elles jouent des rôles multiples et essentiels dans le domaine des données. Elles sont avant tout des productrices de données liées à leur territoire, que ce soit pour leur propre usage, pour l'usage de tiers, ou pour les deux, comme c'est le cas des données d'adresses.

Les collectivités collectent et génèrent une grande quantité de données administratives, qui incluent souvent des informations à caractère personnel, telles que les données des agents publics ou celles nécessaires au fonctionnement des services publics locaux, notamment les services d'état civil. Certaines de ces données, produites par les collectivités, sont destinées à alimenter des référentiels nationaux, tandis que d'autres conservent un usage localisé et plus spécifique au territoire. Cela démontre la pluralité des rôles joués par les collectivités dans la gestion et la production des données, qui sont à la fois locales et d'intérêt national.

[747] Hennion Christine, Altounian Magali et Monthubert Bertrand, op. Cit, p.6.
[748] Ibid.

Selon Frédéric Pointu et Cyril Bras, depuis 2020, les cyberattaques touchent de plus en plus les collectivités territoriales[749] à l'échelle mondiale. Ces attaques, en forte hausse, peuvent aller d'une modification superficielle d'un site web à des perturbations majeures empêchant les collectivités d'assurer leurs missions de service public. Cette tendance inquiétante risque de s'intensifier dans les années futures. Au cours des cinq dernières années, on a observé une hausse significative des cyberattaques à l'échelle mondiale, touchant de plus en plus de collectivités [750]. Parallèlement, les objectifs et le profil des attaquants ont évolué. Ainsi, Pointu et Bras relèvent que ceux-ci ont professionnalisé leurs méthodes et visent désormais principalement les gains financiers. Il est devenu presque systématique qu'une attaque soit suivie d'une demande de rançon ou de menaces de divulgation de données sensibles[751]. Au-delà de l'évaluation correcte de la menace, les contraintes financières représentent un frein majeur à l'intégration généralisée de la cybersécurité dans les collectivités territoriales.

En 2021, la France comptait plus de 45 000 collectivités, incluant communes, groupements de communes et syndicats[752]. Seules les structures les plus grandes disposent des moyens financiers nécessaires pour recruter du personnel spécialisé, essentiel à une protection adéquate. Dans les petites collectivités, il n'est pas rare de voir un seul informaticien, voire aucun, et il arrive souvent que le secrétaire de mairie assume le rôle d'informaticien. Ces personnes sont rarement en mesure de réagir efficacement à une cyberattaque qui pourrait effacer les données numériques de la collectivité. Pourtant, pour la majorité des petites communes, le recrutement d'un expert est quasiment impossible en raison des tensions sur le marché de l'emploi. À cela s'ajoute le fait que, même lorsque les collectivités territoriales parviennent à recruter un Responsable de la Sécurité des Systèmes d'Information (RSSI), elles peinent souvent à les fidéliser. Cette difficulté est due au manque de perspectives de carrière offertes au sein du secteur public, ainsi qu'à des salaires bien inférieurs à ceux proposés dans le secteur privé, rendant ces postes moins attractifs sur le long terme [753].

Les processus de recrutement constituent également un obstacle à l'embauche de RSSI qualifiés. En effet, les grilles salariales des collectivités territoriales sont principalement basées sur le niveau d'études et les années d'expérience dans la fonction publique, ce qui décourage souvent les candidats venant du secteur privé à postuler. Les référentiels métiers du Centre national de la fonction

---

749 Pointu Frédéric et Bras Cyril, « Cybersécurité, résilience et souveraineté dans les collectivités territoriales », Revue défense Nationale, n°855, décembre 2022, pp. 52 – 58.

750 Ries-Marchive Valéry, « Ransomware : la transparence toujours relative des collectivités territoriales », LeMagIT, 29 septembre 2022. www.lemagit.fr/.

751 Pointu Frédéric et Bras Cyril, « Cybersécurité, résilience et souveraineté dans les collectivités territoriales », Revue défense Nationale, n°855, décembre 2022, pp. 52 – 58.

752 « Les collectivités locales en chiffres 2021 ». www.collectivites-locales.gouv.fr/.

753 Loquet Véronique, « Enquête exclusive sur la rémunération des fonctions RSSI », CESIN, 7 octobre 2021 www.cesin.fr/.

publique territoriale (CNFPT), qui régissent les cadres d'emploi, devraient être mis à jour pour mieux refléter les compétences spécifiques recherchées dans le domaine de la cybersécurité, en s'inspirant par exemple du panorama des métiers de la SSI proposé par l'ANSSI[754]. Proposer un plus grand nombre de formations axées sur la sécurité des systèmes d'information (RSSI) à travers le territoire, en privilégiant le recrutement au sein des collectivités territoriales, pourrait constituer une voie intéressante pour améliorer la cybersécurité de nos collectivités à l'avenir. Une autre solution à explorer serait la mutualisation de la compétence SSI entre plusieurs collectivités, permettant ainsi de partager les ressources et les expertises, et d'assurer une protection renforcée, même pour les petites structures disposant de moyens limités. Ainsi, en 2023, les collectivités territoriales restent globalement mal protégées face aux cybermenaces, avec de fortes inégalités territoriales entre celles qui disposent des ressources nécessaires pour assurer leur sécurité et celles qui en sont dépourvues. Toutefois, au-delà des facteurs internes, des éléments externes aggravent également la situation, contribuant à la vulnérabilité de nombreuses collectivités face aux attaques.

Un autre facteur expliquant la hausse des attaques contre les collectivités territoriales est le fait que certaines d'entre elles cèdent aux demandes de rançon [755]. Bien que cette tendance doive idéalement diminuer, payer une rançon, va directement à l'encontre des recommandations de l'ANSSI, désormais de plus en plus largement diffusées auprès des collectivités. L'exemple de la région Normandie, victime d'une cyberattaque fin 2022, illustre bien ce cas : aucune rançon n'a été versée.

En effet, le 8 décembre 2022, le serveur hébergeant l'ensemble de l'infrastructure du portail en ligne de la région Normandie, qui hébergeait également la plateforme GéoNormandie, a subi une attaque informatique. Cette attaque a rendu inopérable la plateforme en ligne jusqu'au 20 avril 2023, soit un peu plus de quatre mois. Un groupuscule de hackers appelé PLAY a ainsi infecté le serveur informatique de la région Normandie en lançant une attaque par rançongiciel. Ces derniers ont ainsi chiffré un certain nombre de serveurs et de postes informatiques, poussant la région à fermer l'ensemble du service informatique [756]. Suite à cela, tous les moyens de communication ont été progressivement coupés, comme le téléphone et le réseau informatique. Tout l'environnement réseau a été coupé, puis progressivement reconstruit grâce à l'aide des experts de l'ANSSI. Les services ont été diversement impactés. Si les services de la CRIGE Normandie ont pu continuer à fonctionner, bien que de façon ralentie, ils n'ont pas totalement cessé, comme le souligne le responsable de la CRIGE Normandie : *« Moi, je travaille surtout avec un réseau, mes outils sont morts, mais ça impacte à peu près 20-25 % de mon travail. Ça ne me bloque pas complètement parce que mes partenaires, eux, n'ont*

---

754 « Panorama des métiers de la cybersécurité », ANSSI. www.ssi.gouv.fr/.

755 Jeunemaitre Julie, « Dans l'oise, les cyberattaques se multiplient dans les collectivités locales : « on a dû payer 10 000 euros de rançon » », France 3, 18 janvier 2021. https://france3-regions.francetvinfo.fr/.

756 Entretien avec le chef du bureau technologie de l'information de la DREAL de Normandie, 13 février 2023.

pas arrêté de travailler. Je peux continuer à travailler sans serveurs, sans annuaires, etc. C'est très pénalisant, mais je peux m'en sortir »[757]. Au contraire, la plateforme GéoNormandie a été entièrement arrêtée durant toute la durée de la crise, comme le souligne son administratrice : *« Tout ce qui est greffé autour de la plateforme : gestion administrative, des adhérents, statistiques, équipe projet, COTEC… Tout se fait dans ce même logiciel qui n'est plus accessible. Ce n'est pas comme si je pouvais me connecter à un site annexe en lien avec GéoNormandie et travailler sur l'administration. Tout se faisait sur la plateforme, donc je n'ai plus accès à l'interne et à l'externe de la plateforme »*[758]. Cependant, malgré ces difficultés, aucune des données stockées n'a été mise en danger, car le serveur contenant ces données était géré sous Linux et les pirates informatiques n'avaient infecté que les ordinateurs équipés de Windows. Une situation qui tend à indiquer que les solutions open source, telles que Linux, sont plus résilientes face à des attaques informatiques que des systèmes plus grand public, comme ceux de Microsoft. La réactivité de l'ANSSI et de la CNIL à la suite de l'annonce de l'attaque informatique et l'efficacité de leur accompagnement auprès de la région Normandie sont également saluées par les responsables de la géoplateforme.

Cependant, la tentation de payer reste forte, surtout pour les collectivités mal préparées. Une attaque réussie, entraînant une fuite des données des usagers ou l'interruption du service public, peut gravement nuire à l'image et à la capacité d'action de la collectivité. Dans ces situations, l'espoir de restaurer rapidement les systèmes d'information en payant la rançon peut peser lourd dans la décision. L'orientation croissante des pirates vers des gains financiers, combinée au fait que certaines collectivités paient, incite davantage ces criminels à cibler ce type de structures.

1.2 Conséquence des attaques ou pourquoi il faut améliorer la protection des collectivités

Le risque de paralysie et de désorganisation de territoires entiers est bien réel. Les collectivités territoriales jouent un rôle essentiel en assurant le bon fonctionnement de la vie quotidienne des citoyens à travers leurs services. En cas de cyberattaque d'envergure et coordonnée, il pourrait devenir extrêmement difficile, voire impossible, de garantir des services fondamentaux, comme la collecte des déchets, le traitement des eaux usées, l'accueil des enfants dans les écoles ou encore la gestion des aides sociales. De plus, les collectivités sont au cœur de la transformation numérique de la société, en développant un nombre croissant de services informatiques destinés aux citoyens. Cependant, cette numérisation amplifie la surface d'attaque, car ces services sont souvent accessibles via internet, exposant ainsi les systèmes aux menaces mondiales. L'importance croissante de ces systèmes

[757] Entretien avec responsable de la CRIGE Normandie, 22 mars 2023.
[758] Entretien l'administratrice de la plateforme GéoNormandie, 22 mars 2023.

numériques signifie qu'une indisponibilité ou une compromission de leur intégrité pourrait entraîner une forte désorganisation et un impact négatif pour les usagers, aggravant ainsi les conséquences d'une cyberattaque.

L'évolution numérique amène les collectivités à centraliser un volume croissant de données personnelles des usagers, certaines étant considérées comme sensibles par la Commission nationale de l'informatique et des libertés (CNIL). En tant que gestionnaires de ces données et représentants de la puissance publique, les collectivités ont la responsabilité d'en garantir la confidentialité. Le cadre réglementaire européen instauré par le RGPD, ainsi que la Loi informatique et Liberté de 1978, impose aux collectivités des obligations de protection toujours plus strictes contre les accès non autorisés, la modification ou la perte de ces informations, sous peine de sanctions financières et d'atteintes à leur réputation. Cependant, garantir la confidentialité ne signifie pas nécessairement assurer la souveraineté sur ces données. En effet, certaines grandes entreprises, notamment américaines, proposent des solutions performantes axées sur le cloud. De plus, plusieurs prestataires cloud américains incluent dans leurs contrats des clauses de licence qui obligent leurs clients à leur accorder un droit et une licence libres de redevance, mondiaux et non exclusifs. Ces droits couvrent l'ensemble des technologies, marques, contenus, informations produites, données, matériaux et autres éléments fournis par le client ou mis à disposition du prestataire cloud. Cette licence est valable pendant toute la durée des droits de propriété intellectuelle du client. Une telle disposition peut soulever des questions importantes en matière de confidentialité, de souveraineté des données et de contrôle sur les informations sensibles, notamment pour des entités publiques ou privées traitant des données critiques, car elle confère au prestataire cloud un accès étendu aux ressources du client, sans contrepartie financière, et ce, à l'échelle mondiale[759]. Cela soulève des interrogations concernant la souveraineté nationale sur les données des citoyens français, notamment en raison de leur soumission à la législation américaine extraterritoriale. De plus, le Code de la commande publique, auquel sont soumises les collectivités, ne considère pas la souveraineté comme une exigence prioritaire. Il faut également noter que plusieurs responsables de systèmes informatiques au sein des collectivités locales dénoncent un certain abandon en matière de souveraineté, concernant les solutions que le Ministère de l'Économie, de l'Industrie et du Numérique leur impose, comme le souligne le responsable informatique de la DREAL de Corse.

> *« Il n'y a pas de réflexion au niveau étatique là-dessus. Niveau souveraineté numérique on revient à du tout privé en ce moment : Microsoft, pare-feux Fortinet. Ça faisait 20 ans qu'on utilisait du Libre Office jusqu'à ce qu'une secrétaire générale décide de faire passer*

[759] KPMG, « Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030 », avril 2021, p. 49.

toute la centrale à Microsoft : c'était il y a 2 – 3 ans. Maintenant ils paient 6000 euros par an pour des licences Microsoft : ça peut provoquer des problèmes quand ils nous envoient des documents. Ce genre de décisions individuelles mettent au panier des décisions de protection informatique vieilles de 20 ans. »[760].

Même remarque à la DREAL de Normandie : *« Nos licences antivirales, on les achète, alors qu'avant le ministère nous les fournissait. Si demain on nous paie la première année et qu'ensuite on nous dit débrouillez-vous, comment va-t-on faire ? »*[761].

Il est également préoccupant de constater que certains décideurs ne sont pas suffisamment sensibilisés aux enjeux de souveraineté, voire sont aveugles à la valeur réelle de ces informations et à leur exploitation potentielle. L'ANSSI a récemment mis à jour une qualification, SecNumCloud, garantissant la sécurité des solutions de cloud en imposant des exigences de cybersécurité et d'étanchéité face aux lois extraterritoriales hors UE.

Face à la montée des cybermenaces, les collectivités territoriales n'ont d'autre choix que de renforcer rapidement leur cybersécurité, car elles constituent une cible privilégiée pour les pirates motivés par le profit. Bien que de nombreux obstacles entravent cette évolution, le niveau de sensibilisation progresse lentement au sein de l'écosystème. Il convient de saluer les initiatives de l'ANSSI, qui, en complément de ses actions de sensibilisation et de qualification des solutions de cybersécurité, pilote un plan de relance cybersécurité pour les collectivités, répondant ainsi aux problématiques financières et facilitant de nombreuses démarches.

Concernant la protection des plateformes d'information géographique, un certain nombre de structures en charge de ces services souffrent d'un manque de moyens humains et financiers chronique. Ainsi, les DREAL qui sont des acteurs importants de la gestion des données géographiques, soulignent souvent des manquements en matière d'investissement dans le domaine de la SSI, en particulier pour les plus petites régions. À titre d'exemple, en 2023 la DREAL de Corse ne pouvait compter que sur trois agents au sein de son unité logistique informatique, qui sont en charge de la protection de l'ensemble du réseau informatique et téléphonique de la DREAL. Aucun poste n'étant spécifiquement dédié à la sécurité informatique [762]. Ce manque de personnel force les responsables informatiques à rogner sur certaines solutions mises en place en matière de sécurité informatique, certaines mesures étant trop complexe pour être gérées par un si petit nombre de personnes, comme la mise en place de listes d'accès ou, par extension, la création de VLAN privé. De plus, la sécurité informatique des DREAL est aujourd'hui dictée par le ministère de l'Économie, de l'Industrie et du Numérique.

760 Entretien avec le responsable informatique de la DREAL de Corse, 6 février 2023.
761 Entretien avec le chef du bureau technologie de l'information de la DREAL de Normandie, 13 février 2023.
762 Entretien avec le responsable informatique de la DREAL de Corse, 6 février 2023.

Cependant les architectures réseau demandées par Paris sont souvent impossibles à mettre en place pour les collectivités qui ne disposent pas des moyens nécessaires à leur application. Cette situation perdure pourtant, malgré les signalements de ces mêmes collectivités. Ainsi, comme l'explique le responsable informatique de la DREAL de Corse,

> *« Aujourd'hui le ministère envoie beaucoup de recommandations, mais ne fait jamais de contrôle sur place, indique de bonnes pratiques de manière générique et laisse les services se débrouiller : on fait ce qu'on veut, mais surtout ce qu'on peut en termes de matériel. Les mises à jour des éléments actifs ne sont jamais vérifiées par les ministères. Le ministère se désengage sur tout, notamment la sauvegarde des données : ils ont déployé le bureau numérique avec des espaces partagés sur le cloud qu'ils gèrent eux, et ils pensent que ça va remplacer tous les serveurs de fichier des DREAL. »*[763].

Les problèmes humains rencontrés par les gestionnaires de réseau ne s'arrêtent cependant pas là. La sensibilisation du personnel des DREAL aux enjeux cyber peut également être laborieuse. Ainsi, malgré la mise en place de sessions de sensibilisation aux attaques informatiques, rare sont les agents à s'y présenter. *« Sur 120 agents il y en a peut-être 20 qui sont venus à cette session d'information »*[764] souligne également le responsable informatique de la DREAL de Corse.

À ces problèmes humains s'ajoutent les problèmes de budget qui freinent le développement de solutions de cybersécurité, en particulier au sein des plus petites collectivités territoriales. *« Le budget dédié à l'informatique correspond à 75 % des besoins de renouvellement que j'ai. Les tarifs des ordinateurs ont augmenté, et tout le monde est équipé en matériel nomade. J'ai besoin de 20 000 euros par an juste pour renouveler le matériel de tous les agents. Il me manque encore 15 000 euros »*[765] indique ce même responsable. Pourtant, les services déconcentrés de l'État, comme les DREAL, veillent sur des éléments comportant un risque potentiel important. Le niveau de supervision imposé par le Ministère, pousse les services SSI à trouver des solutions alternatives, quitte parfois à contourner les mesures imposées par Paris.

> *« Concernant la mise en place du wifi, là aussi on ne pourra pas agir sur les pare-feu, tout sera supervisé par Paris. Il faut qu'on trouve des solutions de contournement. Puisque le contrôleur de domaine est à Paris, en cas de coupure réseau ou de problème de pare-feu, on n'aurait plus moyen d'accéder à nos propres données. Imaginons qu'il y ait un accident sur la centrale thermique d'Ajaccio et que les agents ont besoin d'avoir accès à leur réseau. Le risque est en théorie négligeable, mais, s'il se concrétise, il nous faut quand*

763 Ibid.
764 Ibid.
765 Ibid.

même une solution alternative. On a donc installé un Switch niveau 3 qui fait du réadressage. Pour cela, on doit rebrancher les câbles physiquement »[766].

Afin de répondre à ces problèmes budgétaires régulièrement soulevés par les acteurs locaux, l'État incite les collectivités à passer par le plan France Relance, mis en place à la suite de l'épidémie de Covid en 2020 afin de diminuer l'impact de l'épidémie sur l'économie française. Une solution qui ne peut être au mieux que temporaire, ce programme ayant pris fin en 2022[767]. Cela pose un véritable problème dans le cadre des investissements en matière de cybersécurité. En effet, si des investissements sont faits en se reposant sur France Relance dans le domaine des pare-feux Fortinet imposés par le Ministère, leurs mises à jour à un coût. Lorsque ce dernier ne sera plus pris en charge par le programme France Relance, la question se pose de savoir où les fonds seront trouvés pour maintenir le niveau de protection informatique adéquate sur le long terme.

766 Ibid.

767 Rapport final sur l'évaluation du plan France Relance : https://www.strategie.gouv.fr/publications/comite-devaluation-plan-france-relance-rapport-final

2. L'importance des standards de données

Toutes les administrations publiques produisent des données, et la plupart, à l'exception des plus petites collectivités, les mettent à disposition du public via des plateformes de données dédiées. A priori, cette situation devrait offrir une grande richesse de données disponibles. Toutefois, la mission Data et territoires, remis en septembre 2023, et qui consacre une large part de ses recommandations à la standardisation des données territoriales[768], lève un constat partagé lors des auditions : *« il existe une grande hétérogénéité des données disponibles, souvent accompagnée d'une dispersion des efforts »*[769].

Ainsi, sur un même sujet, deux collectivités peuvent produire des données qui ne sont ni interopérables ni comparables, car chaque collectivité suit ses propres logiques en fonction de ses besoins spécifiques. Cette diversité rend difficile, pour les réutilisateurs, de naviguer dans l'offre de données existante. Lorsque les données ne sont pas uniformément décrites sur l'ensemble du territoire, il devient *« quasiment impossible »*[770] de les agréger efficacement. La mission tient donc la standardisation pour *« un élément essentiel du passage à l'échelle en matière de données »*[771] et insiste sur la dimension collaborative, un standard étant, selon la formule qu'elle reprend à l'observatoire Data Publica, *« à la fois outil et produit de la collaboration »*[772].

Ce constat rejoint directement les enjeux de la normalisation des données géographiques. La constitution de référentiels nationaux complets, qu'il s'agisse de la Base Adresse Nationale, du registre Sirene ou du plan cadastrale informatisé, suppose en effet la contribution d'une multitude d'acteurs publics et privés, que la mission propose d'encouragé par des mécaniques incitatifs, voir par des obligations d'alimentation. Ainsi, elle rappelle qu'un référentiel national n'implique pas nécessairement une base centralisée. En effet, dès lors qu'un standard existe, les données produites localement peuvent être agrégées de manière décentralisée, par moissonnage[773].

Enfin, la mission souligne également deux conditions de passage à l'échelle. La première tient à la traduction des textes juridiques en standards de données, que les textes d'application devraient mentionner explicitement, les collectivités se trouvant le plus souvent *« démunies, faute de doctrine ou d'accompagnement »* face à la multiplication des normes et des réglementations[774]. La seconde concerne le financement : l'appel à projets reste le mode principale de soutien aux initiatives locales.

---

[768] Henion Christine, Altounian Magali et Monthubert Bertrand, « Rapport de la mission Data et territoires », Ministère de la Transformation et de la Fonction publiques, septembre 2023.
[769] Ibid, p.49
[770] Ibid, p.50
[771] Ibid, p.50
[772] Ibid p. 50, citant l'observatoire Data Publica « la standardisation des données ouvertes : favoriser l'interopérabilité, accroître l'impact de l'open data » cahier n°2, novembre 2022, p. 25.
[773] Ibid p. 52
[774] Ibid, p. 52

Toutefois, de nombreux acteurs consultés ont souligné que cette approche tend à mettre en concurrence les territoires pour l'obtention de financements essentiels à la mise en œuvre de leurs projets. Si une certaine concurrence entre territoires, notamment dans le domaine de l'attractivité économique, est compréhensible, cette logique compétitive montre aussi ses limites , d'une part, elle encourage davantage l'élaboration de nouvelles solutions plutôt que la réutilisation de celles qui ont déjà fait leurs preuves ailleurs, car les territoires cherchent à se démarquer par l'innovation, et d'autre part cela tend à mettre les territoire en concurrence et à privilégier l'innovation au détriment de la réutilisation de solutions développés localement, alors que ces problématiques financières appellent justement à la mise en commun des ressources[775].

2.1 Les projets nationaux en matière de normalisation de données géographiques

La normalisation des données géographiques participe également au développement de grands projets nationaux de production de données. Ces projets sont principalement portés par l'IGN qui est en charge du pilotage des projets nationaux de production de données géographiques. Depuis la refondation du modèle de financement de l'IGN en 2020, la construction et le pilotage de grands projets nationaux sont un des leviers les plus importants de financement pour l'Institut, avec la participation aux programmes militaires, tels que Geomaps[776]. Depuis 2020, l'IGN a lancé une série de grands projets nationaux visant à garantir la production de jeux de données sur l'ensemble du territoire national afin d'aider au développement de politiques nationales d'aménagement du territoire. Ces projets sont au nombre de cinq : le Lidar HD (Haute Densité), l'OCS GE, le PCRS, le RPCU auxquels il faut rajouter les projets compris au sein de l'initiative des géocommuns. L'ensemble de ces projets s'articule autour d'un pilotage de l'IGN et une participation des collectivités locales, afin d'élaborer des modèles de données adaptés aux besoins des territoires, mais également pour pouvoir s'appuyer sur l'existant, certains acteurs locaux ayant déjà produit des données similaires à celles développées par les projets nationaux de l'IGN. Derrière cet engagement de l'opérateur national se pose toutefois la question des équilibres de pouvoir et du financement, car la réussite de ces projets dépend étroitement de la participation des acteurs locaux, tant pour la fourniture de données existantes que pour leur cofinancement. La plupart de ces projets reposant pour leur financement sur une mutualisation des moyens d'un grand nombre d'acteurs, mettent également en relief certains problèmes rencontrés lors de l'étape de normalisation des données produites. De fait, la recherche de financement sur laquelle s'appuie l'IGN pour mener ces projets, si elle amène à une consultation accrue des acteurs régionaux et

[775] Ibid. p52
[776] Cf. Chapitre III.

locaux, tend également à raviver les crispations autour de l'étendue des participations financières et de la façon dont sont menés ces projets chez certains acteurs.

En effet, la refonte du modèle économique de l'IGN en 2020, marquée par l'ouverture en open data de la quasi-totalité de ses données et l'abandon du système de revente de données, a contraint l'institut à trouver de nouvelles sources de revenus[777]. Outre les programmes militaires spécifiques, l'IGN mise désormais sur de grands programmes civils cofinancés par l'État et les collectivités pour financer ses missions. Cette dépendance partielle vis-à-vis des financements territoriaux a introduit une logique de négociation et parfois de compétition entre échelons. Comme souligné au chapitre V, les projets nationaux de données géographiques sont devenus le théâtre de tractations sur la répartition des coûts et des bénéfices : ils reflètent les luttes de pouvoir entre les collectivités et l'État, concernant leur pertinence, les moyens qui leur sont alloués et la répartition des tâches. Autrement dit, si tout le monde s'accorde sur l'intérêt général de disposer de référentiels communs (cartographie 3D, cadastre unifié, couverture en imagerie, etc.), des frictions apparaissent quant à savoir qui paie quoi, qui fait quoi, et à quel rythme ces projets doivent avancer.

Le projet de couverture nationale en données Lidar HD, lancé en 2020 est un des plus importants projets d'ampleur nationale créés récemment par l'IGN. Le projet Lidar HD vise à produire une couverture nationale de nuages de points altimétriques par levés Lidar aéroportés à haute densité (10 points/m² en moyenne). Le Lidar HD doit couvrir l'ensemble du territoire national, exception faite de la Guyane, d'ici à fin 2025. Ce projet comporte également un ensemble de jeux de produits dérivés devant accompagner les jeux de données principaux. Il s'agira de modèles numériques de terrain (MNT), modèles numériques du sursol (MNS) et de modèles numériques de hauteurs (MNH)[778]. Les commanditaires principaux de ce projet sont le ministère de l'Agriculture, le ministère de la transition écologique et de la cohésion des territoires, l'Office national des forêts, la Direction Générale de la Prévention des Risques ou encore certaines Régions[779]. Ce projet doit permettre de livrer non seulement une donnée brute disponible en Open Data à travers le portail du site geoservice.ign.fr développé par l'IGN, mais également de traiter les nuages de points obtenus afin d'élaborer des données thématiquement classées répondant à divers besoins de politiques publiques déjà identifiés (prévention

---

777 IGN Institut, « Des données et logiciels ouverts au service de la Nation ». https://www.ign.fr/institut/des-donnees-et-logiciels-ouverts-au-service-de-la-nation. Consulté le 23 mars 2023.

778 IGN, « Point d'information sur le projet de couverture nationale en données Lidar HD », Réunion interrégionale du 15 décembre 2022, p. 1.

779 Les régions et collectivités locales ayant participé au projet dès sa conception sont les suivantes : la Région Occitanie, la Région Sud-Provence-Alpes-Côte d'Azur, et le Département des Alpes-Maritimes. D'autres régions ont rejoins le financement en 2023 comme la Région Grand Est et la Collectivité de Corse à l'aide de subventions du Fonds européen de développement régional (FEDER) d'un montant de 1,3 million d'euros pour la première et de 326 000 euros pour la seconde.

des risques, observation de la ressource forestière, aménagement du territoire…)[780]. La donnée LIDAR HD doit également permettre de fournir une donnée socle en trois dimensions pour le projet de jumeau numérique national soutenu par l'IGN. Le programme Lidar HD est particulièrement ambitieux, et nécessite un financement de près de 60 millions d'euros. 22 millions sont financés par l'État au titre du plan France Relance[781] de septembre 2020. Une subvention du Fond pour le financement de l'action publique [782] a permis de financer les trois premières années du programme à hauteur de 21,55 millions d'euros. Si la Direction Générale de la Prévention des Risques soutient également le programme à hauteur de 4 millions d'euros, le reste du financement se fait en s'appuyant sur les acteurs régionaux et départementaux (soit 12,5 millions d'euros à rassembler). Au 1er juillet 2024, 130 blocs couvrant environ 262 000 km² (48 % de la métropole) sont déjà disponibles en données brutes [783]. À la suite de la mise en place d'un appel à projets par IGNfab dédié aux start-ups et aux PME, quatre projets ont été sélectionnés visant à exploiter les données LIDAR HD nationales. Ces derniers portent sur des domaines aussi variés que les énergies solaires, les surfaces boisées et les massifs forestiers [784]. Cependant, le projet Lidar HD illustre bien un certain nombre de problématiques rencontrées en matière de production de données géographiques sur le territoire, notamment concernant la participation des différents acteurs et les liens entre l'IGN et les collectivités territoriales.

Le nouveau modèle de financement de l'IGN reposant, entre autres, sur la création de grands programmes d'investissement passant par une participation des régions et départements a fini par induire une compétition à la participation financière entre les différentes régions désireuses de bénéficier au plus vite des données Lidar HD. Tout d'abord, si les 60 millions d'euros requis pour le financement de l'ensemble du programme Lidar HD ne sont pas encore réunis, cela ne signifie pas que le programme ne sera pas complété. En réalité, les fonds levés actuellement suffisent à la production d'une première série de données sur l'ensemble du territoire. Aujourd'hui les fonds supplémentaires doivent permettre de garantir la livraison de l'ensemble des produits dérivés promis et éventuellement préparer une mise à jour du programme à l'avenir. Afin de pousser les régions à participer, l'IGN produit les données en priorité sur le territoire des régions contributrices, ce qui explique la répartition des données brutes actuellement disponibles. Cette situation entraîne un certain nombre de frictions, alors que certaines régions ont du mal à débloquer des fonds pour pouvoir participer, d'autres insistent

---

780 IGN Institut, « LiDAR HD : vers une nouvelle cartographie 3D du territoire », 2024. https://www.ign.fr/institut/lidar-hd-vers-une-nouvelle-cartographie-3d-du-territoire

781 Site internet du Ministère de l'Économie : https://www.economie.gouv.fr/plan-de-relance/mesures/doter-france-couverture-lidar-haute-densite-foret

782 Site internet de la direction interministérielle de la transformation publique (DITP) : https://www.modernisation.gouv.fr/actualites/ftap-112-millions-deuros-pour-les-19-projets-laureats

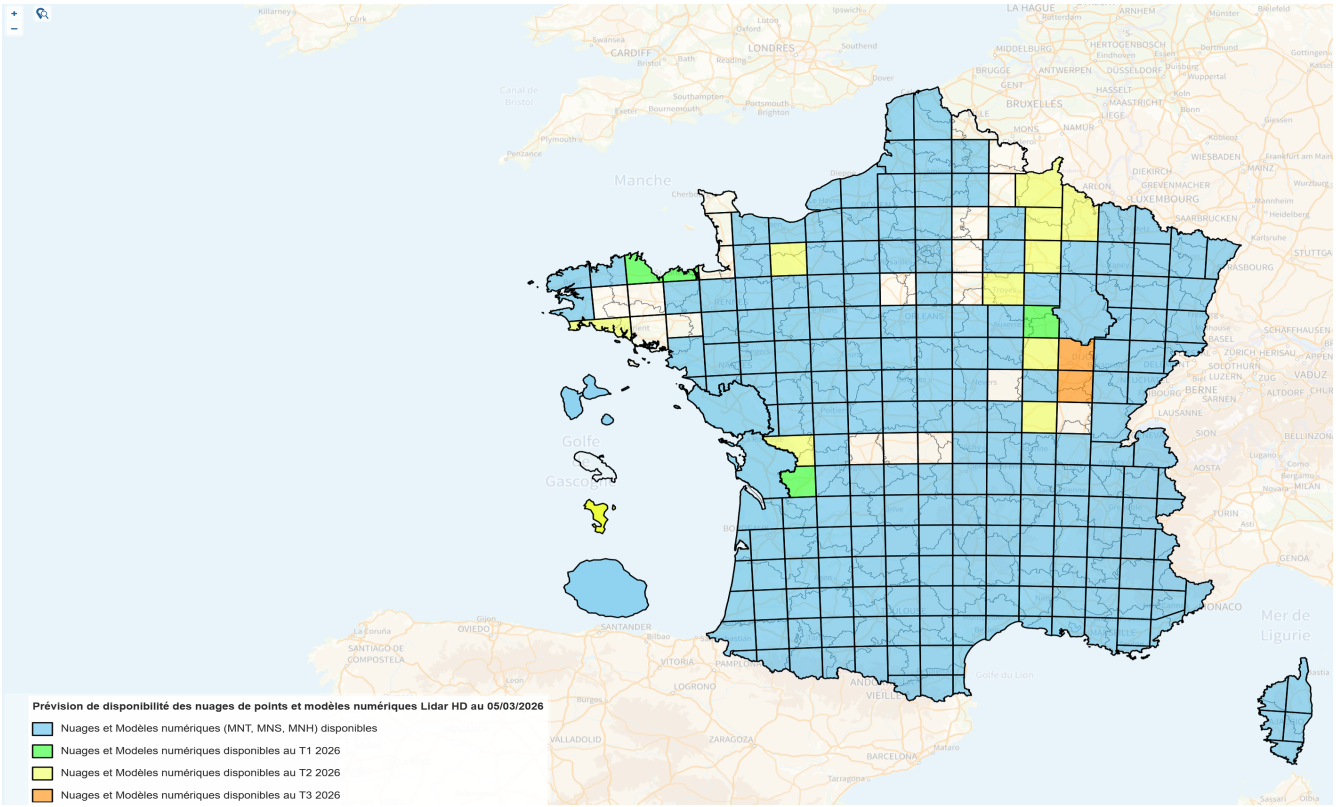
783 IGN, « Les territoires, coproducteurs du référentiel LiDAR HD France entière », Saint-Mandé, 23 novembre 2023, p. 1.

784 Pour une liste complète des projets et des sociétés incubés voir le site d'IGNfab : https://www.ign.fr/ignfab/ignfab-saisons-precedentes

pour dresser une liste des régions participantes ou non et le montant de leurs cotisations, ce que l'IGN refuse, insistant sur la nature volontaire de la participation régionale et départementale [785]. De même, certaines régions développent déjà des projets d'exploitation du Lidar HD, comme la région Hauts de France qui travaille sur un projet de jumeau numérique régional ou encore la région Grand Est. D'autres régions ou collectivités participent au projet en reversant à l'IGN des données Lidar déjà produites sur leur territoire, comme la Région Pays de la Loire ou le Conseil Départemental de la Charente-Maritime. Par ailleurs, la Plateforme DATA du département de la Vendée (Géo Vendée) et l'Observatoire de la côte de Nouvelle Aquitaine (porté par le Service géologique national (BRGM) et l'ONF) se sont également engagés à verser leurs propres données LiDAR au programme national dans une logique de mutualisation de l'action publique [786]. En matière de gouvernance, un comité de gouvernance a été créé rassemblant l'IGN, les ministères participant au financement ainsi que les régions ayant déjà contribué financièrement. Ce mode de gouvernance reflète là encore la mise en concurrence des acteurs locaux. Le comité de gouvernance décide des régions à produire en priorité dans le programme, ce qui explique les zones prioritairement disponibles étaient centré sur le Sud et l'Est de la France, ainsi que le Nord. En 2026 la quasi totalité du territoire métropolitain est couvert (cf. Carte 6).

[785] Propos rassemblés lors de la réunion interrégionale des géocommuns du 15 décembre 2022.
[786] *Ibid*

Carte 6 : Carte de l'avancement des acquisitions LIDAR HD au 5 mars 2026



Source : *IGN Institut (consulté le 5 mars 2026)*

Si ce choix de gouvernance reste rationnel au vu des problèmes de financement du programme complet LIDAR HD, il n'est pas sans conséquence. Toutes les régions n'ont pas réussi à mobiliser les acteurs locaux pour participer au financement du programme, quand bien même les acteurs des plateformes régionales sont conscients des avantages qu'ils pourraient retirer à posséder les données LIDAR sur leurs régions. À ces problématiques financières s'ajoute également le cas particulier des territoires d'outre-mer. Ces derniers, non contents de subir une pression économique forte rendant difficile leur participation [787], sont relégués en fin de calendrier concernant la couverture LIDAR HD. Une situation récurrente dans les programmes de l'IGN du fait des particularités géographiques et climatiques de ces territoires qui rendent les acquisitions de données plus complexes, alors même que la demande est très forte dans ces territoires justement à cause des problèmes très spécifiques qu'ils rencontrent. Le territoire guyanais à ce titre est un exemple parfait, ayant été écarté immédiatement de la première couverture LIDAR du territoire. Une situation qui ne manque pas de faire réagir les acteurs locaux, qui soulignent qu'aujourd'hui la forêt guyanaise reste moins bien connu que la surface de

[787] Les territoires d'outre-mer restent les régions les plus pauvres du territoire d'après l'INSEE. https://www.insee.fr/fr/outil-interactif/5367857/details/territoires/10_ECC/11_ECO/11I_FigureT1

Mars ! Le projet Lidar HD, pourtant porteur d'innovations (donnée 3D libre d'accès, appels à start-ups via IGNfab pour exploiter ces données…), met ainsi en lumière la difficulté de concilier ambition nationale et réalités locales. L'uniformisation technique se heurte à l'hétérogénéité des capacités financières des territoires, et pose la question de la compensation pour ceux qui ne peuvent contribuer autant que les autres. De plus, la nécessité de protéger ces masses de données sensibles ajoute une couche de complexité. En effet, il faut garantir que les nuages de points LIDAR, utiles par exemple pour la prévention des risques ou le déploiement de jumeaux numériques, soient sécurisés contre des usages malveillants, ce qui suppose un haut niveau de confiance entre partenaires et l'application rigoureuse des référentiels de sécurité informatique.

À l'inverse du LIDAR HD, d'autres projets nationaux ont opté pour un financement intégral par l'État, évitant ainsi les frictions liées à l'appel aux fonds locaux. C'est le cas de l'OCS GE. Le projet de référentiel d'Occupation des Sols Grande Echelle (OCS GE) a été lancé à la suite de la publication de la loi climat et résilience d'août 2021[788]. L'objectif de cette loi est d'atteindre un niveau zéro d'artificialisation des sols (ZAN) d'ici à 2050. Le but étant d'atteindre à terme un équilibre entre les flux d'artificialisation et de renaturation des sols sur l'ensemble du territoire. Afin de permettre un suivi national de l'artificialisation des sols et d'aider les collectivités locales à maîtriser leur expansion, le projet d'OCS GE a été lancé par l'IGN et est copiloté par le Cerema et l'Institut national de recherche pour l'agriculture, l'alimentation et l'environnement (INRAE) à la demande du ministère de la Transition écologique et de la Cohésion des territoires. Les bénéfices potentiellement tirés d'une couverture nationale de l'OCS GE sont nombreux, à commencer par la planification des territoires (notamment concernant l'étalement urbain, les portraits de territoires…) et l'aide à l'aménagement de ces derniers (établissement des trames vertes et bleues, définition des aires protégées…). La production de l'OCS GE devra également permettre d'obtenir un référentiel unifié de l'occupation des sols sur l'ensemble du territoire, d'une précision supérieure au référentiel européen Corine Land Cover (CLC) aujourd'hui utilisé. L'OCS GE s'appuie sur des prises de vue aériennes entièrement prises en charge par l'IGN, associé à des modèles numériques de terrain, de surface et à des photographies en infrarouge couleurs (IRC). L'IGN a également développé un outil d'analyse des données brutes s'appuyant sur les capacités de l'intelligence artificielle (deep learning) pour automatiser la télédétection des objets et surfaces, classés en 17 catégories de couverture du sol. Contrairement au projet LIDAR HD, le programme OCS GE est d'ores et déjà financé en intégralité. Son financement est couvert par le Fonds pour la transformation de l'action publique (FTAP) à hauteur de 11 millions d'euros, par le ministère de la Transition écologique et de la Cohésion des territoires (8,5 millions d'euros) et par le ministère de

[788] Loi n° 2021-1104 du 22 août 2021 portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets.

l'Agriculture et de la souveraineté alimentaire (0,5 million d'euros). Son budget global s'élève à 20 millions d'euros. Depuis fin 2025 l'ensemble du territoire métropolitain est désormais couvert (cf. Carte 7). Conformément aux exigences de la loi Lemaire, l'ensemble des données sont diffusées en OpenData par l'IGN.

Carte 7 : Carte de l'avancement de l'OCS GE au 5 mars 2026



Source : *IGN (consulté le 5 mars 2026)*

Cependant, plusieurs problèmes se posent concernant la production d'une norme OCS GE nationale, notamment concernant la coopération État-régions. En effet, l'ensemble des régions et plusieurs métropoles possèdent déjà leurs propres données d'occupation des sols, dont ils ont financé la production et le renouvellement, parfois sans le concours de l'IGN. Ces OCS non normalisés ont été conçus localement afin de répondre aux besoins des collectivités locales concernées. Si les avantages de l'OCS GE sont reconnus par tous, son développement pose de nombreuses questions. Tout d'abord, du fait de l'investissement régional initial dans des OCS propriétaires, les régions cherchent avant tout à se concentrer sur la pérennisation de cette production avant la production de l'OCS GE. De même

l'absence de vision à long terme sur l'OCS GE ne pousse pas les régions à privilégier son déploiement. Si l'objectif annoncé par l'IGN de production de deux millésimes par département d'ici à la fin 2024 est satisfaisant pour une première production, l'actualisation de l'OCS GE au-delà de l'horizon 2025 fait encore l'objet de discussion. Pour résoudre ce problème, l'IGN compte s'appuyer sur une automatisation presque totale du cycle de mise à jour grâce au développement d'outils d'intelligence artificielle qui accompagne le projet OCS GE. Les tests effectués par l'IGN concernant l'IA développée pour l'OCS GE indiquent des résultats tout à fait satisfaisants (plus de 73 % de réussite)[789], mais les contrôles humains restent indispensables pour garantir la qualité de la donnée produite.

La poursuite des mises à jour de l'OCS GE sera donc conditionnée à un rallongement de l'aide financière accordé au projet. Dès la fin du programme initial, il sera urgent de définir si ces financements seront de nouveau accordés par l'État ou non, et sinon comment s'articulera la participation des régions et départements. Tant que des doutes subsisteront, les acteurs régionaux et départementaux continueront à produire leur propre OCS selon leurs besoins. Une telle situation entraînerait un défaut d'harmonisation persistant et un dédoublement des coûts en matière de production de référentiels d'occupation des sols sur tout le territoire, affaiblissant d'autant l'intérêt de l'OCS GE. L'objectif annoncé de la DGALN est de pouvoir mettre à jour l'OCS GE sur l'ensemble du territoire tous les trois ans. Il reste encore à voir si un partenariat durable avec les régions pourra être trouvé pour garantir le renouvellement de la couverture OCS GE. Il est à noter également que la production d'un référentiel national d'occupation des sols ne relève pas réellement d'un besoin exprimé par les régions, mais d'une mesure visant à satisfaire la loi sur l'artificialisation des sols. Aujourd'hui, il existe un risque que se développent en parallèle des bases d'occupation du sol régional décorrélées de la base nationale. Cela pourrait avoir de graves conséquences au niveau local, notamment en entraînant une véritable « guerre des chiffres » entre les élus et les autorités financières. Les régions n'ont pas prévu de financer l'OCS GE aujourd'hui ou dans le futur (pour le moment), ce qui laisse flotter un doute sur les mises à jour de l'OCS GE.

À ces problématiques s'ajoute celle, récurrente, des territoires d'outre-mer. Si, contrairement au projet LIDAR HD, aucun territoire n'est écarté de l'OCS GE, un travail supplémentaire est requis pour pouvoir adapter les outils développés à ces territoires. Le modèle d'IA employé pour la métropole, par exemple, a dû être adapté pour pouvoir analyser les images issues des DROM COM. Ces difficultés placent une nouvelle fois certains territoires ultra-marins en bout de chaîne du programme national, alors même que leurs besoins en matière de référentiels sont plus pressants. À titre d'exemple la Martinique s'appuie encore sur un référentiel BD Ortho de 2017 alors même que le territoire évolue

[789] IGN Institut, « Une carte d'occupation du sol pour faciliter le suivi de l'artificialisation », 4 avril 2024. https://www.ign.fr/institut/une-carte-doccupation-du-sol-pour-faciliter-le-suivi-de-lartificialisation

très rapidement. Pire, les services de santé et les pompiers s'appuient encore aujourd'hui sur cette BD Ortho pour aider la population, car le référentiel de la BD Adresse n'est pas toujours satisfaisant. Les retards accumulés dans ce domaine pourraient avoir à terme de graves conséquences sur la gestion de ces territoires. Cette situation souligne un problème plus large de décalage entre les programmes régionaux d'actualisation des bases de données, comme la BD Ortho et le programme d'OCS GE. Ainsi, dans le cas de l'OCS GE, il s'agit d'une base de données créée afin de lutter contre l'artificialisation des sols, or les mesures à prendre en la matière sont fixées par les SRADDET. Le décalage temporel entre la production de l'OCS GE et la diffusion des SRADDET peut entraîner des problèmes concernant leur applicabilité si la base de données sur laquelle ils doivent s'appuyer est publiée après ce dernier. De même, les SRADDET fixent les objectifs des régions dans plusieurs domaines (infrastructures, mobilités, artificialisation…) qui nécessitent la mise en chantier de programmes basé sur une planification à long terme, comme les SCoT. Les décalages temporels entre les différents programmes nationaux et régionaux entraînent des difficultés en matière de mise en œuvre des projets d'aménagements qui ne peuvent pas s'appuyer sur des données changeantes trop fréquemment. Sur ce point, l'IGN n'est pas à la manœuvre et n'a pas la main sur le déroulement du programme qui est soumis aux impératifs de la DGALN. Un manque de connexion entre besoins nationaux exprimés par des acteurs ministériels et besoins locaux aboutit dans le cas de l'OCS GE à un problème de coordination regrettable pour la bonne marche du projet. Concernant le manque de communication, le lancement de productions départementales dans certains territoires n'a pas toujours été communiqué à la région, qui l'a parfois découvert par voie de presse ou sur les réseaux sociaux.

En matière de normalisation, s'il existe un standard CNIG concernant l'OCS GE, ce dernier ne fait pas l'objet d'une loi ou d'un arrêté et n'a jamais été formellement adopté par l'ensemble des acteurs. Le CNIG continue d'être un intermédiaire important dans le développement de l'OCS GE en offrant une plateforme d'échange, et aide à l'articulation entre les besoins nationaux et régionaux. Dans un contexte où les grands projets nationaux portés par l'IGN dérivent avant tout d'une commande verticale des institutions, notamment ministérielles, la relance du CNIG en 2021 permet d'avancer vers plus de coconstruction de données. On voit bien ici comment la normalisation technique (définir des catégories d'occupation du sol valables partout, grâce à l'IA et la télédétection) est indissociable d'un pilotage politique où l'État joue son rôle d'arbitre de l'égalité territoriale.

Les projets RPCU (Représentation Parcellaire Cadastrale Unique) et PCRS (Plan Corps de Rue Simplifié) s'inscrivent eux aussi dans cette logique de création de « communs géographiques » nationaux, en rationalisant des référentiels jusqu'alors morcelés. Le RPCU consiste à unifier le cadastre en fusionnant les données fiscales (parcelles, propriétés) et les données IGN, afin de disposer d'une carte parcellaire unique sur tout le pays. Il s'agit d'un chantier complexe, mais crucial pour des usages

allant de la fiscalité locale à la gestion foncière ou la planification urbaine. Le PCRS, quant à lui, vise à établir un standard national pour la cartographie à grande échelle du domaine public (voirie, réseaux) en 2D/3D, là où chaque collectivité ou concessionnaire produisait historiquement ses plans selon ses propres méthodes. Ces deux projets impliquent une forte coordination interinstitutionnelle. Le RPCU nécessite un partenariat étroit entre la Direction Générale des Finances Publiques (cadastre fiscal) et l'IGN, tandis que le PCRS mobilise les collectivités, les gestionnaires de réseaux (électricité, eau, télécoms) et l'IGN pour converger vers un référentiel commun. Un rapport sénatorial récent a d'ailleurs souligné ces avancées et appelé à *« Développer, consolider et systématiser les collaborations de l'IGN avec le secteur local »*[790], tout en réaffirmant *« l'importance pour la France de disposer d'un établissement géographique souverain de référence tel que l'IGN »*[791]. Autrement dit, il importe de concilier le maintien d'un pôle national d'excellence (capable de garantir la qualité et la sécurité des données sensibles, d'élaborer des normes, de certifier les productions) avec une gouvernance partagée avec les échelons locaux, ceux-ci étant à la fois co-producteurs et premiers utilisateurs de bon nombre de données.

Le 22 mai 2014, l'IGN, la DGFiP et le Ministère de l'Écologie ont signé une convention afin de produire conjointement la Représentation Parcellaire Cadastrale Unique (RPCU). La RPCU vise à résoudre les problèmes résiduels de discontinuité qui subsistent entre les différentes planches du PCI Vecteur. Les données RPCU des départements 01, 35, 44, 45, 92 et 94 sont aujourd'hui disponibles au format RPCUv1. Depuis 2022 une nouvelle méthode, reposant sur un nouvel outil de rectification des cadastres par le biais d'outils d'intelligence artificielle, a été mise en place par l'IGN, et est testée afin d'accélérer l'harmonisation de la RPCU sur l'ensemble du territoire. L'IGN a soumis un plan de cinq ans pour une production couvrant la France entière. Aujourd'hui, le département de l'Ain (01) est le premier département couvert par le RPCUv2. Cette production doit devenir à terme le nouveau référentiel cadastral national. Cependant, c'est bien à la DGFiP de financer le déploiement du RPCUv2 et de proposer, suite aux résultats de 2023 un plan de financement pour les cinq prochaines années. En dépit de mise en service du RPCUv2, de nombreux doutes subsistent sur le développement du RPCU. Tout d'abord, dans les régions, de nombreuses voix se font entendre et témoignent d'une crispation sur le sujet du cadastre. En cause, principalement le flou général qui persiste sur la poursuite du RPCU et sur le plan qui sera effectivement proposé par la DGFiP. Plusieurs régions doutent que la DGFiP ait les moyens financiers et humains suffisant pour construire ce projet seul. De plus, les régions ayant déjà participé financièrement dans les années 1980 et 2000 à la numérisation du cadastre en données vecteur

[790] Vincent Capo-Canellas, « Acteur de référence de la donnée géolocalisée souveraine, l'IGN avance sur un chemin à baliser », Rapport d'information n° 17 (2022-2023), déposé le 5 octobre 2022, p.16. https://www.senat.fr/rap/r22-017/r22-0170.html.

[791] Ibid, p. 105.

craignent de devoir de nouveau contribuer pour la RPCUv2. Le projet de numérisation homogène du cadastre date maintenant de 20 ans, 15 pour la seule RPCU et la conclusion qui se profile ne plaît guère aux régions.

Un sentiment persistant qui ressort concernant la RPCU ou même d'autres projets, tels que l'OCS GE tient avant tout au fait que ces projets ne viennent pas d'une demande des régions et départements eux-mêmes, quand bien même ils en perçoivent l'utilité globale. Cette forme très verticale de gouvernance concernant ces grands projets nationaux, qui visent avant tout à répondre aux besoins des ministères et du gouvernement, ne rassemblent pas l'adhésion de la majorité des acteurs locaux. Dans le cas de l'OCS GE il s'agit ainsi avant tout de répondre à un besoin d'observation formulé par la DGALN. Le projet LIDAR HD ou encore celui de jumeaux numériques France entière, s'ils sont porteurs de promesses intéressantes en matière d'exploitations, ont été avant tout développé pour enrichir la démarche de suivi de l'anthropocène par l'IGN[792]. Ce mode de fonctionnement rappelle ce qui avait été fait pour la BD Ortho, qui avait été développé avant tout pour répondre aux besoins de la Politique Agricole Commune européenne (PAC), mais en s'appuyant sur des financements locaux. En effet, ces projets se construisant de plus en plus avec la participation financière des acteurs locaux, que ce mode de fonctionnement vertical agace. Il faut ajouter à cela que lorsque des demandes de participation financières sont faites, les régions se retrouvent souvent mises en compétition, comme dans le cas du LIDAR HD. Là encore, cela entraîne de nombreuses frustrations au sein de certaines régions qui manquent cruellement de personnels et de moyens. Bien qu'il arrive également que certaines régions non-contributrices se retrouvent couvertes ou partiellement couvertes, les zones de relevés aériens ne suivant pas exactement les limites administratives. Beaucoup perçoivent aujourd'hui que ce modèle vertical de gouvernance concernant les projets nationaux de production de données géographiques est un peu révolu, et espèrent plus de coproduction dans les données plutôt que de simple appel à participation. Dans le même temps, les projets nationaux d'envergure sont devenus vitaux pour les finances de l'IGN qui se doit de continuer à mobiliser un maximum d'acteurs autour de ces projets qui composent aujourd'hui les fondements de leur financement.

[792] L'Anthropocène est un concept scientifique et politique qui désigne une époque géologique caractérisée par l'impact massif et irréversible des activités humaines sur la planète (changements climatiques, urbanisation, artificialisation des sols, effondrement de la biodiversité, etc.). Dans ce contexte, l'IGN s'est donné pour mission, depuis les années 2020, de documenter, mesurer et représenter les effets de l'Anthropocène sur le territoire français, en tant qu'opérateur public de référence sur les données géographiques. Cette ambition est explicitement formulée dans la stratégie IGN 2021–2025, où il est écrit que l'institut veut *« s'affirmer comme un opérateur public majeur pour la connaissance du territoire à l'heure de l'Anthropocène »*, en produisant des données à très haute résolution, régulièrement mises à jour, et interopérables avec d'autres systèmes (urbanisme, climat, biodiversité, etc.). Source : https://geoservices.ign.fr/sites/default/files/2022-04/Strat%C3%A9gie%20IGN%202021-2025.pdf. Consulté le 2 mars 2024.

L'IGN a pris conscience de ces demandes venant des régions et des collectivités locales sur plus de co-constructions dans les projets nationaux. La création du projet des géocommuns numériques, qui a inauguré la création des réunions interrégionales des géocommuns en décembre 2022 vise également à répondre à ces attentes. Cependant, il faudra que ces réunions se pérennisent dans le temps afin de jouer à plein leur rôle. Des réunions organisées entre les CRIGES et les régions sur l'ensemble du territoire visent aussi à faire remonter au maximum les besoins locaux aux instances de l'IGN ou des ministères. Le CNIG offre également un espace plus horizontal de collaboration en matière de normalisation de ces données. Le CNIG offre un espace de collaboration et permet, dans le cas de projets nationaux, de faire remonter non seulement les besoins, mais également ce qui est déjà produit par les régions, afin d'aboutir à un consensus solide concernant les standards de données. Depuis sa relance post-Covid en 2022, le CNIG est reconnu comme l'autorité principale en matière de normalisation par l'ensemble des acteurs territoriaux et la plupart expriment leur confiance certaine dans la consolidation de son rôle et dans son efficacité à le remplir. Il n'en reste pas moins que certains problèmes persistent. Le CNIG reste à sa source une émanation des ministères et tend à choisir ses ordres du jour concernant la création de nouveaux standards sur la base de leurs besoins. Il n'existe pas encore de mécanisme permettant aux régions ou collectivités locales de faire directement remonter leurs besoins au CNIG. La création des référents régionaux du CNIG depuis 2022 devrait accélérer la circulation des besoins entre les régions et le CNIG à l'avenir. L'application des standards ne donne pas toujours pleine satisfaction. Imposer par la loi l'application de plus de standards peut paraître une solution viable, mais cela ne peut pas être une solution convenable pour l'ensemble des acteurs. Les négociations entourant l'OCS GE sont un bon exemple de cela. Le manque de concertation en amont a fait obstacle au bon déroulement du projet. Parvenir à co-construire les standards et à les rendre acceptables aux yeux de l'ensemble des acteurs du territoire est une condition sine qua non de leur bonne application. La multiplication de standards obligatoires, sans s'assurer au préalable de l'obtention d'un consensus large, risque d'aggraver la situation des régions et de creuser des déséquilibres territoriaux sans résoudre les problèmes d'harmonisation à l'échelle nationale. Cependant, le manque d'obligation rend l'harmonisation au niveau local parfois difficile, comme dans le cas de la constitution des bases de données sur les Espaces Naturel Sensible. La description de ces espaces se fait au niveau départemental et le respect du standard concernant ces espaces, notamment le versant gestion administrative, n'est pas systématique. Cela empêche la fusion de l'ensemble des bases de données départementales et par extension, la constitution de bases de données harmonisées à l'échelle régionale et nationale. La participation équitable des régions et acteurs locaux dans les réunions du CNIG est également sujette à débat. Certains acteurs sont largement surreprésentés (le CNIG, le Cerema, les CRIGEs, ainsi que certaines régions plus investies. Si cette situation souligne un

problème de justice territoriale, il faut tout de même se rappeler que la participation aux groupes de travail et aux réunions du CNIG est ouverte à tous. La motivation et les moyens, à la fois financiers et humains, conditionnent la participation des acteurs locaux, mais tous sont systématiquement invités à participer. De plus, chaque projet de norme s'accompagne d'un appel à commentaire public de plusieurs semaines. Cet appel à commentaire est une étape cruciale de tout projet de normes et voit une participation bien plus variée d'acteurs que les seules réunions du CNIG. Les appels à commentaires constituent de meilleurs indicateurs sur l'implication globale des acteurs publics et privés à tous les échelons du territoire concernant les projets de normes. De plus, le CNIG développe de nouveaux outils visant à faciliter la participation d'un maximum d'acteurs. La diffusion de l'outil GitHub parmi les groupes de travail permet une plus grande ouverture sur le processus de développement des standards et offre la possibilité aux intéressés de poster directement sur le projet GitHub associé leurs questions et suggestions pour l'amélioration du standard. Si la maîtrise de l'outil GitHub n'est pas encore répandue chez tous les acteurs, sa diffusion progressive devrait permettre à terme une plus grande démocratisation de la conception de standards et, à terme, la coconstruction d'un consensus le plus large possible.

Ainsi, en participant à structurer l'offre de données géographique disponible sur le territoire, les standards de données jouent un rôle crucial dans le cycle de production des données géographiques. Reflets des relations parfois tumultueuses entre les collectivités locales et l'État, la production de standard s'appuie sur la participation d'un maximum d'acteurs et mobilise acteurs publics et projets autour de projets communs. Les standards permettent également de mobiliser l'ensemble de la communauté géographique en France et, par la même aide à faire accroître la maturité de ces acteurs sur les enjeux entourant la production et la réutilisation de leurs données. C'est également dans le cadre de ces programmes de normalisation que l'introduction et le développement de normes de protection des données devraient se faire. Ces normes devraient à l'avenir permettre de consolider des mesures bénéfiques en matière de cybersécurité.

Cependant, si l'objectif affiché est bien celui d'une cohérence nationale, les dynamiques observées suggèrent qu'une telle cohérence ne peut être atteinte sans une recomposition en profondeur des rapports entre l'État et les collectivités territoriales. Ces dernières ne sont plus de simples relais locaux de politiques décidées au centre, elles sont devenues des acteurs incontournables de la fabrique de la donnée, capables de produire des informations d'une granularité et d'une actualité souvent supérieures à celles de l'appareil central. Elles jouent un rôle crucial dans la contextualisation, la qualification et l'exploitation opérationnelle des données, notamment dans des domaines comme l'urbanisme, la mobilité ou l'adaptation climatique, où l'expertise de terrain est irremplaçable. De plus, la multiplication des points de production et de circulation de données complexifie considérablement la

gestion de la sécurité informationnelle. L'interconnexion croissante entre systèmes locaux, plateformes nationales et infrastructures européennes accroît la surface d'exposition aux cybermenaces. Dans un tel contexte, la standardisation technique ne suffit plus. Elle doit s'accompagner d'une gouvernance concertée, d'un partage de responsabilités en matière de sécurité et d'une harmonisation des politiques de protection à tous les niveaux. Cette dimension cyber est désormais indissociable de toute réflexion sur la souveraineté géographique. C'est précisément cette question, celle de l'articulation entre ambition nationale et autonomie locale, entre centralisation normative et pluralité territoriale, entre impératif de sécurité et besoin d'agilité, qui constitue le cœur des enjeux à venir. Les grands projets de normalisation ne représentent pas une fin en soi, ils ne sont que les fondations d'un écosystème informationnel pluriel, dont la solidité dépendra de la capacité des acteurs à coopérer, à mutualiser leurs ressources et à construire une gouvernance véritablement partagée. Ainsi, la question de la gouvernance des données et des modalités d'échange entre les collectivités et l'État tient une place capitale dans la façon dont se négocient les rapports de force entre l'État et les collectivités dans la production, l'échange et l'usage de l'information.

2.2 La question de la gouvernance des données dans les échanges entre les collectivités et l'État

Comme le relève le rapport de la mission Data et territoires, aujourd'hui, les collectivités territoriales interagissent avec une multitude d'acteurs qui relèvent du périmètre de l'État[793]. Ces interlocuteurs peuvent inclure divers ministères, agences nationales, services déconcentrés, et opérateurs publics, chacun ayant son propre domaine de compétence. Cette pluralité d'interlocuteurs peut parfois compliquer la coordination des actions et la mise en œuvre des politiques publiques au niveau local. La coordination de l'action de l'État en région incombe d'abord aux préfets, dont le rôle a été réaffirmé par la réforme de l'organisation territoriale de l'État, mais chaque ministère dispose aussi de ses propres services déconcentrés, aux échelons départemental et régional, ce qui accroît la complexité administrative[794].

Cependant, les grands opérateurs de l'État, tels que l'Institut national de l'information géographique et forestière (IGN), l'Agence de la transition écologique (ADEME), le Centre d'études et d'expertise sur les risques, l'environnement, la mobilité et l'aménagement (CEREMA) ou encore l'Office français de la biodiversité, possèdent également des représentations territoriales sous forme de directions régionales ou d'agences locales. Cette multiplicité d'acteurs publics, bien que nécessaires pour couvrir une large palette de missions, peut parfois engendrer une certaine fragmentation, rendant

[793] Hennion Christine, Altounian Magali et Monthubert Bertrand, op. Cit., p. 27.
[794] Ibid

la coordination et la communication plus complexes pour les collectivités locales. L'ensemble de ces acteurs (ministères, services déconcentrés et opérateurs publics) interagissent fréquemment avec les collectivités territoriales sur des questions liées aux données, que ce soit pour leur collecte, leur partage ou leur exploitation. Cependant, comme le souligne la mission Data et territoires, *« la gouvernance actuelle ne semble pas à la hauteur des enjeux liés à l'utilisation optimale des données par les acteurs publics locaux »*[795].

Cette situation se traduit par une fragmentation des initiatives, un manque de coordination entre les différentes entités de l'État et une absence de cadre clair pour l'exploitation harmonisée des données. De nombreuses collectivités, surtout les plus petites, peinent à naviguer entre les différents acteurs et à accéder aux ressources nécessaires pour utiliser les données de manière efficace et stratégique. Un cadre de gouvernance plus intégré, avec des mécanismes de coordination renforcés entre l'État et les collectivités, est nécessaire pour tirer pleinement parti des données dans la gestion des territoires et la mise en œuvre des politiques publiques locales. Cela pourrait inclure des plateformes partagées, des standards de données communs, et un accompagnement accru pour aider les collectivités à développer leurs capacités en matière de gestion et d'exploitation des données. De plus, la mission observe que *« sur un nombre croissant de domaines de l'action publique, il est demandé aux collectivités de transmettre des données »*[796]. Si l'importance de suivre la mise en œuvre des politiques publiques à l'échelle nationale n'est pas remise en question, il n'en reste pas moins que cela constitue une charge significative. Les retours des parties prenantes montrent que cette collecte de données s'opère généralement sans réelle consultation des acteurs impliqués, que ce soit sur les méthodes de collecte ou sur les objectifs visés par celle-ci. Il est important de rappeler que cela découle principalement d'une gouvernance insuffisante dans les relations entre l'État et les collectivités. En l'absence de structures et de mécanismes de concertation véritablement fonctionnels, la transmission de données vers l'État est fréquemment vue comme un processus unilatéral, allant uniquement des collectivités vers les autorités nationales.

La transmission de données de l'État vers les collectivités fait également l'objet de critiques sur deux plans, une situation qui est à la fois relevée par la mission Data et territoires et qui a été confirmé par les entretiens mené par l'auteur. Tout d'abord, sur le plan conceptuel, certains responsables politiques soulèvent une préoccupation : les collectivités sont souvent perçues par les ministères comme de simples fournisseurs de données brutes et consommatrices de solutions numériques clés en main, développées à l'échelle nationale (telles que les plateformes ou les services d'analyse de données). Cela laisse peu de latitude aux collectivités pour exploiter elles-mêmes les données qu'elles

[795] Hennion Christine, Altounian Magali et Monbthubert Bertrand, op. Cit., p. 27
[796] Ibid

collectent et partagent. Il en résulte parfois que des collectivités créent de nouveaux ensembles de données mieux adaptés à leurs besoins spécifiques, ce qui n'est pas optimal financièrement. En fin de compte, l'action de l'État ne favorise pas toujours une plus grande autonomie des collectivités. L'autre reproche porte sur les délais de mise à disposition des données, qui sont fréquemment obsolètes ou dépassées[797]. Ces informations, bien que souvent fournies initialement par les collectivités, sont centralisées au niveau national avant d'être redistribuées (lorsque cela se fait) par l'État. Ainsi, il n'est pas rare de voir des données mises à disposition avec un retard de 2 à 3 ans, bien que des informations plus récentes soient disponibles localement, comme le soulignait le rapport de la mission Data et Territoires, qui cite un témoignage recueilli lors de la rencontre publique organisée par la mission le 8 juin 2023[798]. Or, l'actualisation des données est essentielle pour en garantir une utilisation optimale. Cela concerne particulièrement des secteurs comme la démographie, le vieillissement de la population ou les habitudes de mobilité, où certaines informations datent d'avant 2020, malgré l'impact significatif de la pandémie dans ces domaines. Cette situation est d'autant plus frustrante que l'État s'appuie parfois sur ces données datées pour élaborer et évaluer des politiques locales et nationales, notamment dans l'urbanisme, l'environnement ou la politique de la ville.

En matière de protection informatique, les échanges entre les collectivités et l'État peuvent également être problématiques. Comme le souligne le responsable informatique de la DREAL de Corse, *« La sécurité numérique est prise en compte à différent niveau, mais il n'y a pas de dialogue aux différents niveaux. En service informatique on se retrouve avec des directives qui nous disent de nous débrouiller, c'est nous les responsables. La réflexion globale sur la numérisation de l'État elle est loin d'être faite, chacun joue pour sa paroisse »*[799].

De même, la multiplication des agences et organismes ayant des responsabilités en matière de cyber, pose également question, et le rôle de chacun n'est pas toujours clair. À titre d'exemple, le rôle de la DINUM n'est pas toujours clair aux yeux des agents territoriaux. Les différences de prérogatives entre l'État et la région sont parfois remises en question également. En particulier dans certaines collectivités ou régions dont l'indépendance est jalousement gardée par les acteurs locaux, comme en Corse, et où la communication entre l'État et la région n'est pas toujours aisée. Cette réalité tend à affaiblir les dispositifs nationaux mis en place pour lutter contre les attaques cyber. Ainsi, la création d'antennes régionales de l'ANSSI en Corse va se faire sous l'égide de la collectivité, en effet, un rattachement trop marqué à l'État risque de créer des frictions avec la collectivité dans la gestion des responsabilités de chacun en matière de risque cyber.

---

797 Ibid

798 Ministère de la Transformation et de la Fonction publiques, « Rapport de la mission Data et territoires », septembre 2023, p. 30. https://www.vie-publique.fr/files/rapport/pdf/291763.pdf. Consulté le 23 mars 2025.

799 Entretien avec le responsable informatique de la DREAL de Corse, 6 février 2023.

Ce manque de dialogue et la tendance centralisatrice du gouvernement tendent également à introduire des solutions inadaptées aux besoins des collectivités en matière de protection informatique ou difficilement applicable. Ainsi, le développement de services Cloud par le ministère ne peut pas toujours être mis en place par les collectivités. *« Le ministère nous propose des solutions opaques. Les espaces partagés sur le cloud ne proposent qu'une seule sorte de partage. Si vous accédez au partage, vous avez tous les droits : création, effacement (…) Aujourd'hui les serveurs font l'objet de droits différenciés. Cela reviendrait à créer 200 espaces partagés par métier, ce qui est impossible. Aujourd'hui la solution proposée est inapplicable en l'état »*[800]

souligne le responsable informatique de la DREAL de Corse. La DREAL a ainsi décidé de développer son propre système de sauvegarde sur le Cloud en passant un contrat avec une société monégasque[801]. Ce contrat, entré en vigueur en 2024, lui garantit la sauvegarde de l'ensemble des données gérées par le DREAL, assurant ainsi leur protection, même en cas d'attaque informatique sur le réseau de la DREAL.

Comme nous pouvons le voir, le contexte actuel des interactions entre les collectivités territoriales et les multiples acteurs de l'État met en lumière des défis majeurs liés à la gouvernance, à l'exploitation des données et à la cybersécurité. Si l'État joue un rôle crucial en centralisant des ressources et en proposant des solutions numériques, cette approche centralisatrice montre ses limites face aux besoins spécifiques et souvent diversifiés des collectivités locales. La multiplication des acteurs (ministères, services déconcentrés, agences nationales) complexifie la mise en œuvre des politiques publiques et l'exploitation des données à l'échelle locale. Ce manque de coordination se traduit souvent par une fragmentation des initiatives et des doublons dans les efforts de collecte et de gestion des données. Les collectivités, surtout les plus petites, peinent à naviguer dans ce système et à accéder à des informations adaptées à leurs besoins. Pour améliorer cette situation, il est impératif de mettre en place un cadre de gouvernance clair et intégré. Cela inclut, notamment, la désignation de responsables identifiés pour chaque domaine de données, une centralisation accrue des ressources à travers des plateformes ouvertes et accessibles (comme data.gouv.fr), l'élaboration de standards communs pour garantir l'interopérabilité et éviter les incompatibilités techniques, comme celles rencontrées avec les technologies propriétaires. Ainsi, les collectivités locales se retrouvent souvent dans une relation asymétrique avec l'État, où elles sont perçues comme de simples pourvoyeurs de données. Cette approche empêche souvent les collectivités d'exploiter pleinement les données qu'elles collectent. La mise à disposition tardive ou incomplète des données par l'État accentue cette frustration, notamment dans des domaines où les informations doivent être actualisées régulièrement

[800] Ibid.
[801] Ibid.

(démographie, urbanisme, mobilité…). Pour pallier ces problèmes, il est nécessaire de renforcer les capacités locales grâce à des formations et des financements pour aider les collectivités à développer leurs propres systèmes d'analyse et de gestion des données, et créer des mécanismes de concertation pour inclure les collectivités dans la définition des méthodologies et objectifs de collecte. La cybersécurité constitue un enjeu crucial, mais le manque de dialogue entre l'État et les collectivités affaiblit les dispositifs nationaux. Les solutions proposées par l'État, comme les services cloud centralisés, ne répondent pas toujours aux réalités opérationnelles des collectivités, en particulier celles qui gèrent des environnements complexes. Des exemples, tels que le contrat passé par la DREAL Corse avec une entreprise monégasque pour développer un système de sauvegarde adapté, montrent que les collectivités peuvent innover lorsqu'elles disposent de l'autonomie nécessaire. Cependant, cette approche souligne aussi la nécessité pour l'État de mieux adapter ses solutions aux besoins locaux.

2.3 Les difficultés de l'accès aux données

L'accès et la réutilisation des données publiques ont considérablement progressé grâce à leur ouverture par l'État et ses organismes. Des jeux de données essentiels, tels que le registre des entreprises, le cadastre, les adresses ou encore les transactions immobilières, sont désormais accessibles, alors qu'il était très difficile d'y accéder il y a dix ans. Certains acteurs, comme l'IGN, ont même franchi un cap en rendant l'ensemble de leurs données gratuites en 2021. Cependant, des améliorations sont encore nécessaires, tant pour les données ouvertes que pour celles qui ne sont pas destinées à être diffusées en libre accès. Un problème majeur est la fragmentation de l'offre de données émanant des différents organismes publics. Que ce soit pour une collectivité ou un particulier, il reste complexe d'identifier rapidement les producteurs de données pertinentes dans un domaine précis. Une fois ces producteurs identifiés, il faut encore naviguer entre leurs divers portails. Malgré les efforts de la plateforme data.gouv.fr pour centraliser les données ouvertes, l'ensemble des offres disponibles n'est pas encore pleinement référencé. Le défi principal est donc d'améliorer l'accès aux données et leur visibilité, dans toute leur diversité. La difficulté d'accès aux données est parfois aggravée par la présence de multiples bases de données provenant de différents producteurs traitant du même sujet. La duplication des informations souligne la nécessité d'une gouvernance améliorée et de l'établissement de responsables clairement désignés. De plus, l'interopérabilité entre les référentiels nationaux et les bases de données locales est souvent soulignée comme un objectif crucial par les personnes interrogées. Pour atteindre cette interopérabilité, l'adoption de normes communes est essentielle.

Enfin, on peut observer plusieurs cas où des données utiles étaient disponibles en open data, mais pas organisées selon les découpages administratifs ou zonages appropriés. Il convient de noter que ces zonages sont variés, couvrant des domaines tels que l'urbanisme, la protection de l'environnement ou les politiques urbaines. De ce fait, certains grands producteurs de données, notamment dans les secteurs social ou environnemental, ne peuvent pas fournir les informations à l'échelle correspondant à ces zonages. De nombreuses raisons peuvent entraîner une indisponibilité de certaines données, auprès des plateformes régionales lorsqu'elles sont collectées par d'autres acteurs. Ainsi, l'absence de standards de données peut entraîner une incompatibilité technique entre producteur et diffuseur, et certains acteurs se montrent parfois réticents à partager leurs productions, comme le précise l'animateur du CRIGE Normandie :

> *« Parfois on rencontre des problématiques de partage de l'information avec certains acteurs régionaux : soit pour des raisons techniques, on a des problématiques d'interopérabilité avec nos outils : comme le réseau d'observation du littoral normand-Hauts-de-France, où ils fonctionnent en vase clos. Ils ont leur propre catalogue, mais aujourd'hui, la visibilité de leurs données est assez faible parce qu'ils ont une technologie basée sur ESRI, ce qui crée des problèmes de compatibilité avec GéoNormandie. Des fois on a des problématiques d'acteurs qui sont un peu timorés sur l'ouverture et la diffusion de leurs données »*[802].

Le problème de la rétention des données est un problème rencontré dans toutes les régions et par l'ensemble des plateformes régionales d'informations géographiques. Certains acteurs n'ont pas nécessairement développé une culture de l'ouverture de leurs données, même dans le cas de partenariats nationaux. Ainsi, toujours dans le cas de la plateforme GéoNormandie, *« Je trouve que le monde de la recherche est assez fermé, peut-être parce qu'on ne va pas assez vers eux et eux vers nous. Certains laboratoires universitaires de hauts rangs, qui sont membres de la CRIGE, notamment dans le cadre des travaux sur le changement climatique, ce n'est pas toujours évident de récupérer leurs données. Peut-être qu'on n'a pas assez l'habitude de travailler ensemble. »*[803].

Le cas du développement du référentiel régional pédologique (RRP)[804] au sein de la région Normandie, avant et après la fusion des deux précédentes régions (Haute et Basse Normandie) en une

---

802 Entretien avec l'animateur de la CRIGE Normandie, 22 mars 2023.

803 *Ibid*

804 Le référentiel pédologique français est une classification élaborée dans les années 1980 sous l'égide de l'Association française pour l'étude du sol et de l'INRA qui remplace la classification des sols CPCS mise au point de 1964 à 1967 par la Commission de Pédologie et de Cartographie des Sols (CPCS). Source : Pan Ming Huang, Yuncong Li, Malcolm E. Sumner, *Handbook of Soil Sciences*, CRC Press, 2011, pp. 32-16.

seule, est symptomatique des problèmes rencontrés par certaines géoplateformes lorsqu'elles doivent récupérer des données produites par d'autres acteurs.

> *« Les RRP étaient régionalisés avec un RRP haut normand et bas normand. La diffusion du RRP haut normand ne pose aucune difficulté. Le RRP bas normand pose des difficultés puisqu'ils n'avaient pas intégré sa diffusion dans le montage du projet. On a un acteur associatif qui a mené la constitution de ce RRP, on a rencontré des problèmes. Il n'y avait pas de notice. Le RRP haut normand avait prévu une notice dès sa conception, ce que n'avait pas prévu le RRP bas normand. Un RRP sans notice n'est pas forcément utilisable ou interprétable. Assez symptomatique de la façon dont le projet a été mené à l'époque en région Basse-Normandie, avec un acteur qui fonctionne presque comme une entreprise privée. La fourniture de service autour de la donnée fait partie de son activité. Pour la Haute-Normandie le conservatoire des espaces naturels a rendu ces données accessibles de façon complètement ouverte. »*[805].

Ces freins en matière de communication constituent aujourd'hui une cause importante de l'appauvrissement de certaines bases de données géographiques. Une situation d'autant plus dommageable, que de nombreuses données existent déjà, mais ne peuvent pas être exploités. Si ce manque de communication peut être dû à un manque de connaissance entre certaines acteurs, il est clair que certaines communautés ne tiennent pas à ce que leur données soient diffusés de façon ouvertes. Certaines craignent un manque à gagner en termes de profit, tandis que d'autres sont plus réticentes pour des raisons plus politiques. Par exemple, le pilote des systèmes d'information de la DREAL de Bretagne n'hésite pas à évoquer le cas de certaines données sensibles dans le domaine de l'agriculture :

> *« En Bretagne il y a une question sur l'agriculture, publier les données, ça peut être perçu comme alimenter l'agro-bashing. Il pourrait y avoir une position claire indiquant que les données doivent être rendues accessibles. Cela permettrait à l'administration de mieux cibler les contrôles, notamment concernant les règles sur l'abattage des porcs, mais, d'un autre côté cela permettrait à l'administration d'aller voir les endroits où il faudrait vraiment aller voir et ça, ça pose des problèmes. La position de la DREAL sur ce sujet a été de rechercher la facilité administrative en demandant que le nombre de cochons dans les installations soit communiqué en temps réel afin de ne cibler que les installations qui pourraient poser problème. Mais le nombre de cochons n'est pas communiqué. Je ne suis même pas sûr que le ministère de l'Agriculture le connaisse. On préfère aujourd'hui avoir une complexité administrative parce que ça permet à beaucoup de passer au travers des*

[805] Entretien avec l'animateur de la CRIGE Normandie, 22 mars 2023.

contrôles de l'administration. On est pas du tout dans un cas de transparence où vous pouvez connaître les endroits où a lieu l'abattage des cochons ou non »[806].

Ainsi, la diffusion des données géographiques ne va pas toujours de soi, et certains acteurs gardent jalousement leurs données ou cherchent à ce que certaines ne soient pas communiquées au public, de peur des retombés négative que cela pourrait engendrer à leurs yeux. Le fonctionnement en silo de certains organismes qui considèrent les données qu'ils produisent comme leur monnaie d'échange ne tend pas non plus à faciliter la diffusion des données. Ainsi, malgré la mise en place de politiques publiques dédiés à l'open data et la diffusion de standards de données visant à accélérer la circulation des informations, il reste encore du chemin à parcourir avant que l'ensemble des données utiles collectées par les producteurs de données puissent être librement communiquées. Au-delà des questions de sécurité et de confidentialité propres aux enjeux entourant la défense nationale, certains intérêts politiques et personnels s'opposent encore aujourd'hui à une circulation plus vaste des informations géographiques auprès des citoyens.

L'ouverture des données publiques a marqué une avancée significative, offrant un accès élargi à des informations essentielles, comme le cadastre, les adresses ou les transactions immobilières. Ces progrès, notamment avec des initiatives telles que la gratuité des données de l'IGN depuis 2021, illustrent une volonté de rendre les données plus accessibles. Cependant, des obstacles persistent, notamment la fragmentation de l'offre, la duplication des bases, et des problèmes d'interopérabilité technique entre les différents acteurs. Un des défis majeurs reste la mise en place de standards communs pour garantir la compatibilité entre les référentiels nationaux et locaux. L'absence de normes harmonisées aggrave la complexité d'intégration, comme illustrée par les problèmes rencontrés avec le réseau d'observation du littoral Normand-Hauts-de-France, où les technologies propriétaires (comme ESRI) limitent la visibilité et l'accessibilité des données. De même, le cas du Référentiel Régional Pédologique (RRP) en Normandie met en évidence des disparités dans les pratiques de collecte et de diffusion. L'absence de documentation standardisée ou d'engagement dès le départ pour une diffusion ouverte nuit à l'exploitation des données par des tiers. Ces cas soulignent l'importance d'une gouvernance renforcée et d'une coopération accrue entre les acteurs publics et privés. Au-delà des aspects techniques, des barrières culturelles freinent encore l'ouverture des données. Certains acteurs, notamment dans le milieu universitaire ou associatif, hésitent à partager leurs productions, invoquant des raisons liées à la propriété intellectuelle ou à un manque d'habitude de collaboration. Ces réticences, bien que compréhensibles, ralentissent les dynamiques d'innovation et de valorisation des données. Pour répondre à ces défis, une meilleure centralisation et une gouvernance collaborative sont

[806] Entretien avec le pilote des systèmes d'information de la DREAL Bretagne, 20 février 2023.

nécessaires. La plateforme data.gouv.fr, bien qu'efficace, ne parvient pas encore à référencer l'ensemble des jeux de données disponibles. L'amélioration de cette centralisation, associée à une coordination plus étroite entre les plateformes locales et nationales, est essentielle pour éviter la duplication des efforts et optimiser la visibilité des données. Malgré ces limites, des initiatives comme l'ouverture totale des données de l'IGN ou la promotion d'interopérabilité par des standards internationaux (tels que ceux de l'OGC ou de l'ISO) montrent que des progrès sont possibles. Les bénéfices de ces démarches sont multiples : une meilleure prise de décision pour les politiques publiques, une stimulation de l'innovation dans les secteurs privé et académique, et un renforcement de la transparence et de la participation citoyenne.

Ainsi, l'ouverture des données publiques et la mise en place de standards communs pour l'interopérabilité sont des étapes clés vers une meilleure gestion et exploitation des informations géographiques. Cependant, malgré ces avancées, l'optimisation et l'intégration de ces données restent des défis majeurs, notamment pour leur usage dans des technologies émergentes. Parmi ces innovations, le concept de jumeau numérique (JN) représente une nouvelle approche prometteuse pour la modélisation et la gestion des territoires. En s'appuyant sur des données géographiques, des modèles 3D et des technologies avancées comme l'Internet des objets (IoT) et l'intelligence artificielle, les jumeaux numériques ouvrent la voie à une planification plus efficace et à une prise de décision optimisée. Toutefois, leur déploiement soulève également des défis en matière de structuration, de normalisation et de traitement des données, illustrant ainsi l'importance d'une gouvernance cohérente et d'une interopérabilité renforcée.

3. Entre interconnexion, innovation et risque cyber : étude de cas du projet de jumeau numérique des territoires (JNFT)

Le jumeau numérique (JN) est une technologie émergente entourée de nombreuses promesses et susceptible de remodeler l'avenir des industries et de la société dans son ensemble. La définition la plus fréquente du Jumeau numérique peut être présentée de la façon suivante. Selon Grieves[807], qui a forgé ce terme en 2002, le concept de jumeau numérique trouve son origine dans la gestion du cycle de vie des produits. Si ce concept est appliqué aux données géographiques, aux modèles et aux métadonnées, ceux-ci peuvent être décrits sur la base d'un cycle de vie du produit. Le cycle de vie d'un produit décrit la somme des phases individuelles par lesquelles un produit passe tout au long de son cycle de vie. Par

[807] Grieves M., « Digital twin: manufacturing excellence through virtual factory replication: a whitepaper », 2014.

conséquent, outre la description détaillée des données géographiques et des modèles de données (via les métadonnées), leur cycle de vie est également décrit. Ainsi, le développement des différents composants du jumeau numérique (bâtiments, routes, etc.) peut être planifié et mis à jour numériquement, et peut être renouvelé ou entretenu sur la base d'un intervalle défini. Un JN est donc un système de systèmes qui va bien au-delà des simulations et analyses informatiques traditionnelles. Il s'agit d'une réplique de tous les éléments, processus, dynamiques et microprogrammes d'un système physique dans un équivalent numérique [808]. Les deux systèmes (physique et numérique) existent côte à côte, partageant toutes les entrées et les opérations en utilisant des communications de données et des transferts d'informations en temps réel. Grâce à l'intégration de l'internet des objets (IoT), de l'intelligence artificielle, des modèles 3D, des communications sans fil de nouvelle génération (5G/6G), de la réalité augmentée, de la réalité virtuelle, des capteurs électroniques, l'homologue numérique/virtuel du système réel est en mesure d'assurer une surveillance, une analyse, une évaluation et des prédictions sans faille. Un JN offre une plateforme pour tester et analyser des systèmes complexes, ce qui serait impossible avec les simulations traditionnelles. Cependant, le développement de cette technologie est confronté à de nombreux défis. Il y a, entre autres, la complexité d'une communication efficace et de l'accumulation de données, l'indisponibilité de certaines données pour former des modèles d'apprentissage automatique, le manque de puissance de traitement pour prendre en charge des jumeaux de haute fidélité, le besoin élevé de collaboration interdisciplinaire et l'absence de méthodologies de développement et de mesures de validation normalisées. En réalité, à l'heure actuelle, il n'existe aucun JN réellement complet d'une ville et encore moins d'un pays entier. La plupart des JN existant en France, comme à l'étranger, sont des JN dits « locaux » (JNL), tels que définis par la Commission européenne [809]. Un jumeau numérique local est une sous-catégorie de JN axée sur les villes ou les environnements urbains. Un JNL reproduit numériquement une zone géographique spécifique (par exemple, une ville, un quartier ou une infrastructure municipale) afin d'améliorer la planification urbaine, la gestion des ressources et la prise de décision au niveau local. Alors qu'un JN peut théoriquement modéliser n'importe quelle entité physique à n'importe quelle échelle, un JNL est limité à une région géographique particulière et se concentre principalement sur les défis et les applications liés à la gouvernance locale, à la durabilité et au développement de villes intelligentes.

Les JN sont apparus comme un ensemble de technologies expérimentales permettant de reproduire les éléments, les fonctions, les opérations et la dynamique des systèmes physiques dans le

[808] B. R. Barricelli, E. Casiraghi, et D. Fogli, « A survey on digital twin : definitions, characteristics, applications, and design implications, », 2019.

[809] https://digital-strategy.ec.europa.eu/en/library/local-digital-twins-forging-cities-tomorrow

monde numérique, avec un meilleur contrôle des essais, de l'analyse, de la prédiction et de la prévention des risques pour les processus sensibles [810]. Toutefois, jusqu'à récemment, les technologies de soutien n'étaient pas suffisamment avancées pour développer des réseaux communs pour des systèmes complexes ou des systèmes de systèmes. Les développements récents en matière d'apprentissage automatique, d'intelligence artificielle, d'intégration des données, de réalité virtuelle/augmentée, de détection, de sécurité et de stockage sur le cloud, ont permis la mise en œuvre du JN et de ses applications étendues dans plusieurs secteurs. Un des secteurs clés qui s'est emparé de la problématique des jumeaux numériques est celui de l'aménagement du territoire, en particulier dans les environnements urbains [811].

La formation d'une image miroir d'un système physique dans le monde numérique offre de nombreuses possibilités. L'interconnexion des systèmes physiques et numériques par le biais d'un transfert de données permet au système virtuel d'exister en même temps que le système physique. Les communications de données en temps réel entre les systèmes physiques et numériques permettent un fonctionnement synchronisé et cohérent des systèmes physiques et virtuels. Une fois dans le domaine numérique, l'apprentissage optimisé, le transfert d'informations, l'analyse, la visualisation, l'optimisation et la planification peuvent facilement être incorporés pour voir les améliorations potentielles avec les changements suggérés. Ainsi, le JN peut être utilisé efficacement pour produire des simulations détaillées du système physique, suggérer des changements et visualiser les améliorations potentielles. En France, plusieurs métropoles disposent déjà de leurs propres jumeaux numériques reposant sur une maquette 3D[812]. Dans la plupart des cas, ils servent à communiquer avec les citoyens sur des projets d'aménagement, mais restent en général assez peu intégrés aux processus métier des services des métropoles, notamment en raison de leur manque d'interopérabilité avec les outils existants. Les jumeaux les plus avancés permettent d'intégrer et de visualiser des résultats de simulations, sur quelques thématiques d'intérêt, mais de nombreux services techniques disent être trop dépendants des bureaux d'études (capables d'initier des simulations) pour les phases de pré-étude. Les JNT déployés en France couvrent très majoritairement des zones urbaines et ne permettent pas d'appuyer les décisions d'aménagement en zone rurale, alors que ces territoires sont sujets à des évolutions tout aussi complexes (risques naturels, évolution des paysages, développement économique, gestion des ressources…) et que des interactions existent entre l'urbain, le péri-urbain et le milieu rural.

---

[810] M. Grieves et J. Vickers, « Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems, » in *Transdisciplinary perspectives on complex systems*, pp. 85–113, Springer, 2017.

[811] Schrotter Gerhard et Hürzeler Christian, « The Digital Twin of the City of Zurich for Urban Planning », pp. 99-112, Springer, 2020.

[812] Egis Conseil, « Miroir, miroir… : le jumeau numérique du territoire », La Banque des Territoires, p. 9, juillet 2021.

L'adoption de projets de jumeaux numériques territoriaux ne se fait cependant pas toujours sans heurts. Ces derniers mettent en jeu de nombreux acteurs aux intérêts divergents, ce qui engendre des rivalités sur la gouvernance des données. La collecte et diffusion des données géographiques est ainsi un domaine de concurrence entre les autorités gouvernementales cherchant à conserver leur rôle de garants de l'intérêt public d'une part, le secteur privé qui collecte/exploite des données à des fins commerciales d'autre part, et les communautés prônant l'ouverture des données. Ainsi, certains acteurs peuvent retenir leurs données plutôt que de les partager, ce qui freine l'exploitation de bases de données existantes et la construction de jumeaux numériques réellement fédérateurs. Ces divergences reflètent des idéologies opposées, avec d'un côté l'importance de la souveraineté des données du point de vue de l'État, et de l'autre l'ouverture/démocratisation des données au bénéfice de l'innovation collective. Un point de vue défendu par certains acteurs régionaux. Trouver un équilibre entre protection, partage et souveraineté est un enjeu clé pour les jumeaux numériques de territoires. Deux grandes approches technologiques, voir idéologiques, s'opposent dans la mise en place des jumeaux numériques de territoire. D'une part, une stratégie « clés en main » portée par de grands éditeurs de logiciel propose des plateformes propriétaires complètes, mais souvent peu ouvertes. D'autre part, des approches fondées sur l'interopérabilité et l'open source misent sur des solutions modulaires conçues sur mesure. Ce choix technologique crée des rivalités entre partisans de chaque camp

Les Jumeaux Numériques Territoriaux (JNT) connaissent une adoption croissante en France, principalement dans les métropoles. Des villes pionnières ont choisi des plateformes propriétaires existantes. Ainsi, Rennes a été la première ville à mettre en œuvre un jumeau numérique en 2017, en collaboration avec Dassault Systèmes[813], s'inspirant du projet pionnier de Singapour, Virtual Singapore, lancé en 2015[814]. Depuis, d'autres villes françaises, telles que Lille, Angers (avec le soutien de Siradel), Lyon, Brest, et Aix-Marseille (en partenariat avec Geofit) ont suivi cette dynamique. Ces initiatives s'appuient sur des cas d'usage variés, notamment la communication sur les projets d'aménagement, l'identification des îlots de chaleur urbains, la gestion du risque d'inondation et la création de cadastres solaires pour optimiser le déploiement de panneaux photovoltaïques [815]. Cependant, ces solutions offrent une mise en œuvre rapide avec des usages déjà développés, mais au prix d'une dépendance technologique (formats propriétaires, licences coûteuses) et d'une interopérabilité limitée. Cette logique « boîte noire » peut entrer en conflit avec les principes d'ouverture et de transparence chers à certains

[813] Richard Marin, « Ces villes créent des jumeaux numériques pour améliorer leur qualité de vie », Le Figaro immobilier, 4 février 2023. https://immobilier.lefigaro.fr/article/ces-villes-creent-des-jumeaux-numeriques-pour-ameliorer-leur-qualite-de-vie_c3483442-a318-11ed-b0cc-f4f42454a73a/

[814] Egis Conseil, « Miroir, miroir… : le jumeau numérique du territoire », La Banque des Territoires, p. 9, juillet 2021.

[815] Géoservices, « Retour sur l'appel à communs pour la conception du Jumeau numérique de la France et de ses territoires », 29 novembre 2024. https://geoservices.ign.fr/actualites/2024-11-jumeaux-numeriques

acteurs publics[816]. Les maquettes 3D de ces jumeaux numériques sont parfois enrichies par des données dynamiques issues de capteurs IoT ou de services techniques. L'agrégation et le traitement des données nécessaires à ces applications sont facilités par des acteurs comme Hexagon, Siradel, et IGO[817]. Certaines villes connectées choisissent de valoriser principalement des données métier (gestion des déchets, infrastructures, réseaux), souvent sans s'appuyer sur des modèles 3D. À titre d'exemple, 1Spatial propose des outils spécialisés pour les collectivités afin de gérer efficacement ces données métiers. D'autres collectivités privilégient une idéologie de souveraineté numérique en construisant leur jumeau numérique sur des bases ouvertes. À titre d'exemple, Strasbourg Eurométropole, a refusé le modèle 100% propriétaire. Dès 2018, Strasbourg a misé sur l'open source et des standards ouverts, comme OpenBIM pour la modélisation des bâtiments, pour bâtir progressivement son jumeau[818]. La collectivité a d'abord défini ses usages prioritaires, puis acquis seulement les données et outils indispensables, en privilégiant des logiciels libres ou interopérables adaptés à ses besoins. Cette approche a permis à la ville de conserver la maîtrise technologique locale de son Jumeau et d'éviter le verrouillage par un seul fournisseur. Comme l'explique le responsable SIG de Strasbourg Olivier Banaszak[819], utiliser de l'open source demande un investissement, mais cela permet de mutualiser les avancées entre territoires et de garantir une plus grande équité d'accès aux innovations, même pour les collectivités aux moyens limités. Chaque approche à donc ses mérites, indépendance technologique contre facilité d'implémentation, mais découle de choix politiques précis qui mettent à jour des luttes de pouvoir entre deux visions idéologiques distinctes entre ouverture et service sur étagère.

Un autre foyer de rivalité concerne la place du secteur privé dans la « ville intelligente » et les jumeaux numériques, notamment en France où certaines métropoles ont confié leur projet à des consortiums privés. Ces projets suscitent des débats idéologiques sur le contrôle public des infrastructures numériques versus leur délégation à des acteurs privés. Ainsi à titre d'exemple, l'agglomération d'Angers Loire métropole a lancé en 2020 l'un des projets de jumeau numérique de territoire les plus ambitieux de France, confié à un groupement mené par Engie[820]. Le jumeau numérique d'Angers comprend l'installation de 50 000 capteurs IoT et d'un hyperviseur urbain centralisé pour optimiser les services municipaux, comme l'éclairage, le trafic routier, ou encore la

---

816 Egis Conseil, « Miroir, miroir… : le jumeau numérique du territoire », La Banque des Territoires, p. 34, juillet 2021.

817 Josse Fanny et Riss Sylvain, « Le jumeau numérique environnemental » à l'échelle du territoire, les données au cœur des cas d'usage », EDP Science, 2024. https://www.shs-conferences.org/articles/shsconf/pdf/2024/18/shsconf_edubim2024_03003.pdf

818 Egis Conseil, « Miroir, miroir… : le jumeau numérique du territoire », La Banque des Territoires, p. 35, juillet 2021.

819 *Ibid.*

820 Petitjean Olivier, « Géants du numérique, privatiseurs et marchands d'armes : pourquoi la révolte couve contre la « smart city », Observatoire des multinationales, 27 février 2020. Disponible ici : https://multinationales.org/fr/enquetes/villes-contre-multinationales/geants-du-numerique-privatiseurs-et-marchands-d-armes-pourquoi-la-revolte-couve. Consulté le 23 aout 2025.

gestion des déchets. Ce choix a toutefois généré des controverses, ainsi d'un point de vue économique, certains ont questionné la rentabilité réelle du dispositif high-tech, évaluant que son coût (178 millions d'euros sur 12 ans) n'était compensé que par environ 100 millions d'euros d'économies potentielles sur 25 ans. Autrement dit, la solution technologique pourrait ne pas « se payer elle-même », et des critiques y voient une préférence idéologique pour la technologie coûteuse au détriment de solutions politiques alternatives plus frugales pour atteindre la neutralité carbone. Surtout, ce modèle soulève la question de la dépendance vis-à-vis d'un prestataire privé. En effet, en confiant la gestion numérique de la ville à Engie & partenaire, la collectivité risque d'enraciner la privatisation de fonctions urbaines stratégiques. Des experts soulignent que les données et le « savoir-faire » accumulés par le prestataire pourraient, à terme, rendre la ville captive. Ainsi, si Angers voulait reprendre la main plus tard, le déséquilibre d'information profiterait au consortium privé[821]. Cette tension oppose une vision libérale à une vision souveraine où la ville garde la maîtrise de ses infrastructures numériques et de ses données.

Enfin, au-delà de la France, des rivalités idéologiques fortes sont apparues dans certains projets emblématiques à l'étranger, notamment autour de la protection de la vie privée et de la gouvernance urbaine. Un cas souvent cité est celui de Sidewalk Labs (filiale d'Alphabet/Google) à Toronto, au Canada. En 2017, Sidewalk a proposé de développer un jumeau numérique d'un quartier (Quayside) pour en faire la smart city du futur, hyperconnectée. Très vite, le projet a provoqué un tiraillement entre la vision technologique de Google et les exigences des acteurs publics et citoyens en matière de contrôle démocratique. Tout d'abord, Les autorités canadiennes et la société civile ont craint que le projet ne débouche sur une « ville privée » gérée par une entreprise tech, où la collecte massive de données envahirait la vie quotidienne. Plusieurs experts membres du projet ont démissionné avec fracas, dénonçant l'absence de garanties suffisantes pour la protection des données et de la vie privée des citoyens[822]. Cette fronde interne a braqué l'attention du public sur les intentions réelles de Sidewalk Labs. Le conflit s'est aggravé quand Sidewalk Labs a dévoilé une première ébauche de son plan directeur en 2019. L'entreprise y apparaissait extrêmement ambitieuse. En effet, elle souhaitait s'étendre bien au-delà du terrain initialement concédé, contrôler elle-même la construction et l'exploitation de tout le quartier, conserver la propriété exclusive des technologies et des données urbaines collectées, et même obtenir un statut réglementaire d'exception pour déroger aux lois existantes. En clair, Google imaginait un quartier où elle ferait la loi, hors du cadre municipal habituel. Cette vision d'une ville gérée comme une plateforme privée a déclenché une levée de boucliers des autorités locales, des habitants et d'associations. Face à ces réactions, une confrontation s'est engagée entre Sidewalk Labs et les garants de l'intérêt public. Finalement, le projet a dû être fortement révisé.

821 *Ibid.*
822 *Ibid.*

Ainsi, le gouvernement a imposé un retour à un périmètre plus restreint, a interdit à Sidewalk Labs d'être l'opérateur unique du quartier et a exigé la création d'un organisme public indépendant pour gérer les données urbaines collectées, afin que celles-ci restent une ressource commune et non la propriété de Google. Cette capitulation partielle de Sidewalk, suivie quelques mois plus tard de l'arrêt complet du projet par Alphabet en 2020, incarne la rivalité idéologique entre deux modèles de ville avec d'un côté, la « smart city corporatiste » pilotée par un géant du numérique, et de l'autre la « ville intelligente démocratique » où la collectivité conserve la maîtrise des règles du jeu et des données.

Outre les métropoles, des initiatives locales se développent également sur des territoires plus vastes. À titre d'exemple, le port de Bordeaux a créé un jumeau numérique de l'estuaire de la Gironde pour effectuer des simulations hydrodynamiques, tandis que la Vendée utilise une maquette 3D pour établir un cadastre solaire et planifier le déploiement de panneaux photovoltaïques [823]. Dans l'Aude, une maquette en maillage 3D est utilisée pour des études paysagères et la gestion des risques naturels [824]. Des entreprises comme VorteX-IO, Bluemapping, et Predict Services (en partenariat avec IGO) proposent des solutions innovantes pour l'anticipation des inondations et la gestion de l'eau, renforçant ainsi les capacités des communes à se préparer et à gérer les crises [825].

D'autres applications des jumeaux numériques incluent la simulation de mobilité. Des entreprises comme Aimsun[826] et Insight Signals[827] offrent des solutions exploitant des données granulaires pour réaliser des études d'impact dans des contextes variés. Ces technologies s'avèrent précieuses pour optimiser les flux de circulation et planifier de nouveaux aménagements urbains. Par ailleurs, des acteurs tels que la société montpelliéraine Bionatics[828] ou encore la société Ndunes[829] se spécialisent dans la modélisation 3D des paysages, facilitant la communication autour de projets d'aménagement, notamment dans les domaines des énergies renouvelables et des infrastructures. En plus des métropoles, les jumeaux numériques intéressent également les acteurs industriels. En France, la SNCF développe un jumeau numérique de son réseau ferroviaire, couvrant les ouvrages d'art et la signalisation, dans le cadre d'un projet financé par la BPI pour optimiser la gestion des ponts

---

[823] Beltran Jacques, « Les jumeaux numériques pour moderniser les villes de demain », Dassault Systems, BatInfo, 4 février 2024. https://batinfo.com/tribune/les-jumeaux-numeriques-pour-moderniser-les-villes-de-demain_27543

[824] IGO, « Jumeau numérique du Département de l'Aude – GEODATADAYS 2022 : Un autre usage des données PCRS pour répondre aux enjeux régionnaux et ruraux », 2022. https://www.igo.fr/laval-virtual-et-geodatadays-2022/

[825] RVI, « Villes immersives : Jumeaux numériques à la rescousse ! », 30 septembre 2024. https://www.crvi.ca/villes-immersives-jumeaux-numeriques-a-la-rescousse/

[826] https://www.aimsun.com/fr/aimsun-insight/

[827] InsightSignal, « In Aulnay-sous-Bois, a Digital Twin for urban mobility developed by Insight Signals », 21 février 2023. https://insight-signals.com/region-ile-de-france-2/

[828] https://mybionatics.com/landsim-3d/

[829] Pignon Jean-Christophe, « Un quartier d'Épinal modélisé en 3D grâce à une technologie innovante », Vosges matin, 1er juin 2023. https://www.vosgesmatin.fr/economie/2023/06/01/un-quartier-d-epinal-modelise-en-3d-grace-a-une-technologie-innovante

ferroviaires [830]. De son côté, la société RTE (gestionnaire du réseau de transport d'électricité en France) modélise le réseau de transport d'électricité pour tester des scénarios complexes, tels que l'arrêt d'une centrale ou la rupture d'un câble [831]. Dans le secteur logistique, des entreprises comme CMA-CGM créent des modèles numériques détaillés pour leurs chaînes logistiques, intégrantes des données en temps réel issues de capteurs pour optimiser les opérations et simuler des perturbations potentielles [832]. Ces multiples initiatives montrent que les jumeaux numériques ne se limitent pas à la gestion urbaine. Ils s'étendent à des secteurs stratégiques, comme l'industrie, les transports et la gestion des ressources naturelles, faisant de cette technologie un outil prometteur pour répondre aux défis de demain.

Cette situation a poussé l'IGN, le Centre d'études et d'expertise sur les risques, l'environnement, la mobilité et l'aménagement (Cerema) et l'Institut national de recherche en informatique et en automatique (Inria), à lancer la démarche « Jumeau numérique de la France et de ses territoires » en 2022. L'objectif est de déployer une démarche et l'outillage numérique nécessaire pour fédérer les initiatives locales et permettre le passage à l'échelle des jumeaux numériques de territoires, dans un cadre de coconstruction public-privé et État-collectivités. Le projet de jumeau numérique de territoire (JNT) vise à mutualiser les données géospatiales et à développer une plateforme ouverte et interopérable, favorisant ainsi des collaborations public-privé. En s'appuyant sur des outils avancés, tels que les simulations IA et les technologies immersives, le JNFT porté par l'IGN ambitionne de répondre à des défis multithématiques, allant de la gestion des risques à la planification écologique. Cependant, si ce projet est prometteur, il fait face à de nombreux défis. La gouvernance des données est un enjeu important pour l'ensemble des acteurs impliqués dans ce projet. À cela s'ajoutent également des défis en matière d'interopérabilité des données [833] et de cybersécurité afin de garantir la protection des données une fois le jumeau numérique mis en place.

---

830 SNCF, « SNCF Réseau leader dans le BIM et le jumeau numérique du système ferroviaire », SNCF Numérique, 6 décembre 2022. https://numerique.sncf.com/actualites/sncf-reseau-leader-dans-le-bim-et-le-jumeau-numerique-du-systeme-ferroviaire/

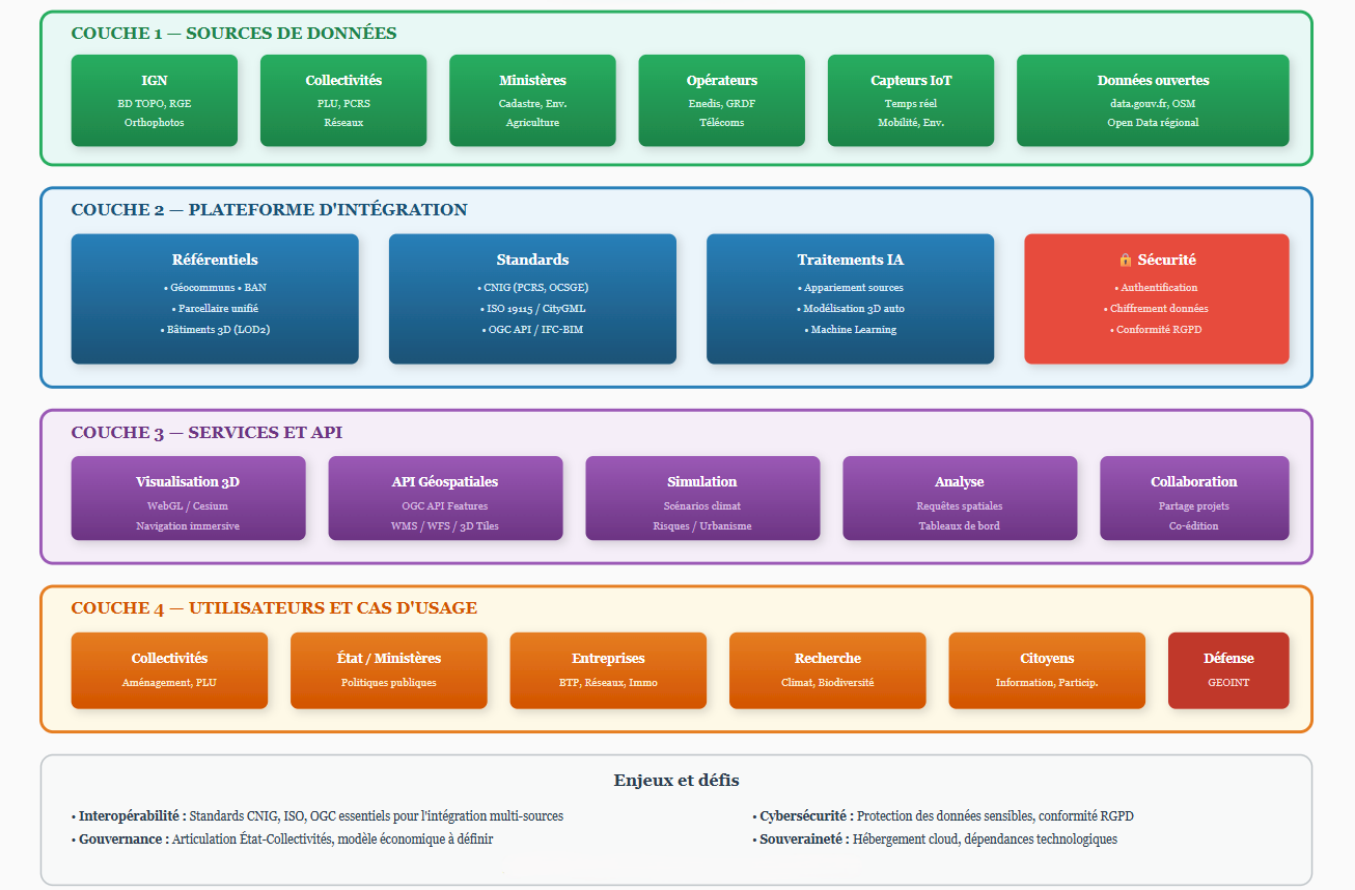
831 Raoul Gaëtan, « Jumeau numérique : pour RTE, le jeu en vaut la chandelle », LeMagIT, 17 juin 2021. https://www.lemagit.fr/etude/Jumeau-numerique-pour-RTE-le-jeu-en-vaut-la-chandelle

832 CMA CGM, « RAPPORT RSE 2023 : Déclaration de performance extra-financière », p. 38, 2023. https://www.cmacgm-group.com/api/sites/default/files/2024-02/CMA%20CGM_Rapport%20RSE%202023_Web%20(1).pdf

833 Devilliers Olivier, « L'interopérabilité, enjeu central du jumeau numérique national », 2 juin 2024. https://www.banquedesterritoires.fr/linteroperabilite-enjeu-central-du-jumeau-numerique-national

3.1 Le Jumeau numérique des territoires : un programme prometteur qui fait face à de nombreux défis

Figure 18 : Architecture du Jumeau Numérique de la France et des Territoires (JNFT)



Source : *IGN et enquête de terrain de l'auteur*

S'il existe déjà en France plusieurs initiatives en matière de jumeaux numériques, ces dernières restent, pour la majorité, concentrées dans quelques grands territoires urbains. Ces jumeaux numériques, bien qu'innovant, sont souvent développés pour des usages spécifiques, limités à des thématiques isolées, comme la gestion des infrastructures ou les projets d'aménagement. Cette approche monothématique, combinée à des outils rarement interopérables et à des données sous-exploitées, limite leur portée et freine leur potentiel d'innovation. De nombreux JNT fonctionnent encore en silo, ce qui entraîne une duplication des efforts et des coûts élevés. Pour dépasser ces

limitations, l'Union européenne, à travers l'initiative EDIC Local Digital Twins towards CITIverse[834], promeut la mutualisation des ressources et des connaissances. Une telle approche permettrait de développer des solutions à grande échelle, tout en réduisant les coûts de recherche et de maintenance. Elle introduirait une interopérabilité entre les systèmes et encouragerait le partage de briques technologiques pour éviter les redondances. Ce modèle, basé sur la collaboration, stimulerait l'innovation et favoriserait la diffusion des savoirs entre acteurs publics et privés. Si l'établissement d'un jumeau numérique européen reste encore loin, les principaux défis, pour la France, comme les autres pays européens, sont déjà clairement énoncés. L'interopérabilité et la collaboration entre structures publiques et privés sont au cœur du projet de JNFT.

C'est dans cette perspective que s'inscrit le projet de JNFT. En croisant les données et les expertises, le JNFT a le potentiel de devenir un outil systémique au service des territoires. Il ambitionne d'offrir une infrastructure socle, pensée pour faciliter l'accès au marché aux startups et PME innovantes, tout en les aidant à développer des outils et services à forte valeur ajoutée. Le rapprochement entre la recherche et l'industrie, encouragé par le JNFT, doit également permettre à terme de surmonter les verrous technologiques actuels, notamment en matière d'interopérabilité et de sécurité, et d'accélérer la mise sur le marché de solutions innovantes. En parallèle, le JNFT doit permettre de structurer et soutenir une véritable filière économique française autour du géonumérique, en rassemblant les acteurs de plusieurs secteurs stratégiques, comme le géospatial, la data, l'intelligence artificielle et les infrastructures cloud. Une telle infrastructure devra permettre de réduire considérablement les coûts initiaux associés au développement et à l'utilisation des JNT. Dans l'idéal, cette réduction des coûts permettra aux entreprises, notamment les startups et PME, de se concentrer sur l'aval de la chaîne de valeur, favorisant ainsi des applications plus diversifiées et accessibles.

Le projet JNFT attire d'ores et déjà l'intérêt de nombreux grands utilisateurs et entreprises de premier plan, positionnant ainsi le projet comme une initiative d'envergure nationale. Parmi les partenaires en discussions avancées figurent des acteurs majeurs, tels que SYSTRA, Egis, Suez, Vinci Concessions, Artelia, EDF Renouvelables, AXA Next, Enedis, et Bouygues[835]. Des opérateurs de réseaux et des acteurs territoriaux, tels que SNCF Gare & Connexions, Société des Grands Projets (SGP), HAROPA port, GRDF, MAIF, Colas, et Icade manifestent également un fort intérêt [836]. L'objectif annoncé par l'IGN est aujourd'hui de garantir leur participation active dès le lancement prévu pour le deuxième trimestre 2025, notamment à travers leur implication dans la gouvernance du

---

834 DÉCISION D'EXÉCUTION (UE) 2024/459 de la Commission du 1er février 2024, sur la création du consortium pour une infrastructure numérique européenne intitulé « Networked Local Digital Twins towards the CitiVERSE » (EDIC LDT CitiVERSE). Https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202400459

835 IGN, « Jumeau numérique de la France et des territoires : Dossier de candidature à France 2030 », p. 10, novembre 2024.

836 *Ibid*

projet. De plus, la plateforme JNFT se destine à devenir avant tout une plateforme technique sur le mode PaaS (Platform as a Service). Cette dernière doit avant tout constituer un socle commun sur lequel viendront se connecter des projets et technologies développés par les différents acteurs. Ces derniers pourront ainsi profiter à leur tour des données mis à disposition par les acteurs étatiques pour développer leurs outils, en faire la promotion et dégager un profit à la suite de leur investissement initial dans le développement de la plateforme.

À ce jour, le consortium du JNFT réunit 13 partenaires stratégiques [837]. Parmi eux, l'IGN et le Cerema, deux opérateurs publics majeurs, jouent un rôle clé dans l'acquisition, la modélisation et l'expertise des données territoriales, notamment dans les domaines des transitions écologique, climatique et énergétique. Le projet bénéficie également de la contribution de quatre institutions de recherche de premier plan : Inria, LASTIG (UGE-ENSG), CNES, et IFPEN. Ces acteurs apportent leurs compétences dans l'acquisition et la visualisation des données géographiques, la modélisation 3D, ainsi que la simulation de systèmes complexes. Sur le plan industriel, le consortium inclut six entreprises spécialisées dans la production de données géospatiales et les technologies associées : 1Spatial France, Camptocamp, Siradel, IGO-Geofit, LuxCarta, et GeometryFactory. Ces acteurs combinent leurs expertises complémentaires pour couvrir tout le spectre des besoins technologiques liés aux jumeaux numériques. Enfin, Cap Digital, pôle de compétitivité national dédié aux technologies et aux usages numériques, est chargé d'animer et de structurer la filière géonumérique, notamment autour des données et de l'intelligence artificielle.

Peut également être cité ici l'appel à communs, organisé de mai à septembre 2024 par l'IGN, le Cerema et l'Inria. Ce dernier à recueilli 200 réponses, dont 50 provenant de collectivités territoriales, avec toutes les échelles représentées, régions, départements, métropoles, EPCI, communes, et 80 réponses d'entreprises [838]. Cet appel à communs a permis d'initier un écosystème national d'acteurs publics et privés concernés par ces technologies numériques et services de simulation offerts par les jumeaux numériques de territoires. Pour garantir la réussite du projet, le consortium propose ainsi une gouvernance élargie, impliquant progressivement des directions d'administrations centrales, des collectivités territoriales, des opérateurs de plateformes régionales, ainsi que des entreprises et acteurs scientifiques. Cette gouvernance vise à intégrer toutes les parties prenantes dans les orientations stratégiques du projet et dans son exploitation industrielle. Cette première phase de consultation a notamment permis de souligner certains problèmes auxquels le JNFT devra faire face pour qu'il soit une réussite. Le besoin de mutualisation des coûts notamment, est un problème de premier plan. Enfin,

---

[837] Les 13 membres du consortiums sont les suivants : IGN, Cerema, Inria, LASTIG (ENSG Géomatique), CNES, IFPEN, 1Spatial, CamptoCamp, SIRADEL, IGO, Cap Digital, Geometry Factory et LuxCarta.

[838] Géoservices, « Retour sur l'appel à communs pour la conception du Jumeau numérique de la France et de ses territoires », 29 novembre 2024. https://geoservices.ign.fr/actualites/2024-11-jumeaux-numeriques

même si de nombreux acteurs industriels ont manifesté leur intérêt, leurs compétences sont très spécialisées : data science, géomatique, modélisation 3D, BIM, gestion des risques, aménagement… Mais il n'existe pas pour le moment de proposition croisant plusieurs thématiques métier qui s'appuierait sur des données géographiques partagées. Le manque d'interopérabilité entre les différents acteurs reste un des plus gros défis à relever.

Le projet Jumeau numérique de la France et des Territoires (JNFT) implique donc une collaboration complexe entre un large éventail d'acteurs publics et privés, chacun ayant des intérêts, des priorités et des perspectives spécifiques. Cette diversité d'acteurs soulève des défis importants en matière de gouvernance, qui doivent être adressés pour garantir la réussite et la pérennité du projet. Ces défis se décomposent en plusieurs dimensions, allant de la coordination organisationnelle à la gestion des droits sur les données. Le JNFT regroupe des acteurs variés, tels que des institutions publiques (IGN, Cerema), des organismes de recherche (Inria, CNES), des collectivités locales, ainsi que des entreprises privées de toutes tailles. Ces acteurs ont souvent des objectifs distincts : les acteurs publics se concentrent sur des missions d'intérêt général, comme la transition écologique et l'aménagement du territoire, tandis que les entreprises privées cherchent des opportunités économiques et des retours sur investissement. Assurer la pérennité non seulement technologique, mais également financière du projet est aujourd'hui une priorité, afin de garantir la participation d'un large spectre d'acteurs, pour que le poids financier de la participation ne constitue pas un frein trop important pour les collectivités locales ou les petites et moyennes entreprises.

Le marché des données géospatiales reste largement méconnu, malgré son fort potentiel et sa croissance constante. Ce terme désigne l'ensemble des activités économiques liées à la collecte, la production, le traitement, l'analyse, la distribution et la visualisation de données géoréférencées. Il englobe à la fois les technologies matérielles et logicielles, les services associés (comme le conseil, l'analyse ou l'ingénierie) et les applications finales dans des domaines aussi variés que l'urbanisme, la défense, la logistique, l'environnement, l'agriculture, la santé ou la sécurité[839]. En France, ce secteur dynamique regroupe environ 2 000 entreprises, dont 1 500 françaises et 500 étrangères, qui fournissent leurs services à 400 entreprises et institutions nationales d'après la dernière enquête de l'Afigéo[840]. Avec des revenus annuels cumulés estimés entre 6 et 11 milliards d'euros, le marché français se décompose en trois segments principaux : la surveillance et l'observation (satellite, aérien, lidar, drone : 1,6 milliard d'euros), le positionnement GNSS (6,6 milliards d'euros) et l'analyse et la visualisation

[839] Geospatial World, « GeoBuiz Global Geospatial Industry Outlook 2022 », 2022. Disponible ici : https://geospatialworld.net/consulting/reports/geobuiz/2022/index.html#download-ebook. Consulté le 2 mars 2025.

[840] Afigéo, « Etude complète économique écosystème Géonumérique », septembre 2024, p. 90. https://www.afigeo.asso.fr/wp-content/uploads/2024/09/16/etude-economique-ecosysteme-geonumerique-afigeo.pdf. Consulté le 3 mars 2025.

des données (3,08 milliards d'euros)[841]. Au niveau mondial, le marché géospatial représentait environ 372 milliards de dollars en 2024, avec une croissance annuelle de 14 %. L'Europe compte pour 25 % de ce total (93 milliards de dollars), derrière les États-Unis (111 milliards)[842]. Entre 2016 et 2021, ce marché a connu une progression de 71 %, et les projections annoncent une accélération : il pourrait atteindre 712 milliards de dollars en 2025 et dépasser 1 300 milliards de dollars d'ici 2030[843]. Parallèlement, le marché des jumeaux numériques (tous secteurs confondus) affiche une croissance exceptionnelle. Selon Fortune Business Insights, sa valeur devrait passer de 16,55 milliards d'euros en 2024 à 242 milliards d'euros d'ici 2032, avec une croissance annuelle moyenne de 36 % [844]. Le segment des services est particulièrement porteur, représentant plus de 60 % des revenus attendus en 2030[845]. Cette filière emploie environ 70 000 experts dans le pays[846]. Son poids économique direct est estimé autour de 10 milliards d'euros annuels (soit près de 9 % de l'économie numérique française). Si l'on prend en compte l'ensemble des services reposant sur la géolocalisation (tourisme, mobilité, etc.), l'impact économique indirect du secteur atteindrait même 35 milliards d'euros.

En France, le développement des jumeaux numériques bénéficie d'une attention accrue, notamment dans le cadre du rapport interministériel « Mission exploratoire sur le métavers »[847]. Celui-ci souligne l'opportunité de structurer une filière nationale compétitive, impliquant startups, PME, ETI et grands industriels. Déjà, de nombreuses entreprises développent des jumeaux numériques thématiques et des outils aval : entrepôts de données, outils de simulation et de visualisation. Cependant, leur adoption reste freinée par leur complexité et leurs coûts initiaux élevés, souvent portés par les entreprises, alors que la création de valeur se concrétise principalement en aval.

---

841 Euroconsult, « Space Economy Report », 2023 cité dans « Étude économique de l'écosystème géonumérique en France », Afigéo, p. 47, septembre 2024. https://www.afigeo.asso.fr/wp-content/uploads/2024/09/16/etude-economique-ecosysteme-geonumerique-afigeo.pdf. Consulté le 3 mars 2025.

842 *Ibid*

843 Geospatial World, « Advancing & Augmenting USD 1.4 Trillion Geospatial Market by 2030 », 2023. https://geospatialworld.net/gw-market-insights/advancing-augmenting-usd-1-4-trillion-geospatial-market-by-2030/

844 Fortune Business Insight, « Geospatial Imagery Analytics Market Size, Share & COVID-19 Impact Analysis, By Imaging Type (Video and Image), By Collection Medium (Geographic Information System (GIS), Satellite Imagery, and Others), By Application (Weather Conditions Monitoring, Disaster Management, Urban Planning/Development, Natural Resource Exploration, and Others), By End-user (Defense & Security, Healthcare, Retail & Logistics, Government, Banking, Financial Services & Insurance (BFSI), Mining/Manufacturing, Agriculture, and Others), and Regional Forecast, 2023-2030 », 2024. https://www.fortunebusinessinsights.com/geospatial-imagery-analytics-market-108685

845 GlobalData, « Digital Twin Market Trends and Analysis by Region, Product and Service, End-use and Segment Forecast to 2030 », 31 janvier 2023. https://www.globaldata.com/store/report/digital-twin-market-analysis/

846 IGN Mag, « Géonumérique, la filière qui valait 10 milliards », 30 septembre 2024. https://www.ign.fr/mag/geonumerique-la-filiere-qui-valait-10-milliards. Consulté le 3 mars 2025.

847 Basdevant Adrien, François Camille, et Ronfard Rémi, « Mission exploratoire sur les métavers », octobre 2022, p. 9. https://www.economie.gouv.fr/files/files/2022/Rapport-interministeriel-metavers.pdf

3.2 Le Jumeau numérique des territoires au défi de la normalisation des données

Le JNFT fait également face à un défi de taille concernant les nombreux besoins en matière de normalisation des données. Ces besoins sont accentués par les développements à l'échelle européenne et internationale, où l'ambition serait à terme de pouvoir créer de véritables jumeaux numériques transnationaux, notamment à l'échelle de l'Union.

Ainsi, à l'échelle européenne, des initiatives, telles que Destination Earth[848], un jumeau numérique de la Terre axé sur les enjeux climatiques, offrent des capacités de simulation à une échelle planétaire. Ces projets démontrent l'importance d'aligner les résultats des simulations globales avec des outils plus locaux pour rendre ces données exploitables à des niveaux régionaux ou municipaux. L'initiative EDIC Local Digital Twins[849] vise également à opérationnaliser plus largement les jumeaux numériques, favorisant des synergies entre projets nationaux et européens, notamment via des plateformes comme le JNFT, qui peut valoriser ces éléments au sein d'un réseau collaboratif international. Ce consortium, dont la France est membre fondateur par l'intermédiaire du Cerema, prévoit de fournir aux collectivités européennes une boîte à outils d'interopérabilité basée sur la norme NGSI-LD[850]. En s'appuyant sur les spécifications développées au sein de l'EDIC, le JNFT devrait adopter les standards promus au sein de ce consortium pour garantir une meilleure interopérabilité entre les jumeaux numériques déployés en France et leurs homologues européens. De plus, des mécanismes d'interopérabilité minimale (MIM), comme le MIM 7, employé au sein du programme EDIC, facilitent l'orchestration des traitements distribués et les échanges de données entre jumeaux numériques européens [851]. Cette interconnexion facilitera les échanges de données et la coordination des initiatives transfrontalières. Un autre projet majeur, Digital TER-X 2050[852], se concentre sur la création d'un cadre européen pour les espaces de données dédiés au secteur de la construction. Ce projet vise à promouvoir une gestion des ressources plus durable, en s'appuyant sur

[848] https://digital-strategy.ec.europa.eu/en/policies/destination-earth

[849] https://digital-strategy.ec.europa.eu/en

[850] NGSI-LD est un modèle de données et une API pour la publication, le requêtage et l'abonnement aux informations de contexte. Il vise à faciliter l'échange ouvert et le partage d'informations structurées entre différentes acteurs, dans des domaines d'application tels que les villes intelligentes, l'industrie du futur, l'agriculture numérique, et plus généralement pour l'internet des objets, les systèmes cyber-physiques, et les jumeaux numériques. Source : ETSI, « Context Information Management (CIM) ; Information Model (MOD0) », 2019. https://www.etsi.org/deliver/etsi_gs/CIM/001_099/006/01.01.01_60/gs_CIM006v010101p.pdf

[851] Union Européenne, « Minimal Interoperability Mechanisms: Advancing Europe's digital future », 26 août 2024. https://data.europa.eu/en/news-events/news/minimal-interoperability-mechanisms-advancing-europes-digital-future

[852] https://digitalter-x.eu/what-is-digital-ter-x-2050/

les jumeaux numériques et l'infrastructure Gaia-X[853], pour réduire les émissions de CO2 et améliorer la transparence des processus de construction. Cette initiative ambitionne de transformer profondément le secteur en intégrant des technologies avancées pour une meilleure efficacité et une empreinte carbone réduite. Gaia-X, qui s'inscrit dans les priorités de la transition numérique et climatique de l'UE, alimente également les ambitions du Pacte vert pour l'Europe en renforçant la résilience environnementale et la durabilité des politiques européennes.

À l'échelle internationale, plusieurs pays développent des projets nationaux de jumeaux numériques. Les Pays-Bas[854], par exemple, ont créé un modèle vecteur 3D de tous leurs bâtiments pour des usages comme la gestion des risques de submersion, en partenariat avec des entreprises telles que Sogelink. Au Royaume-Uni[855], une initiative nationale rassemble des secteurs industriels impliqués dans les jumeaux numériques, bien qu'il n'existe pas encore de plateforme centralisée. Le Japon, avec son projet Plateau lancé en 2020[856], se concentre sur l'aménagement urbain et la résilience aux tremblements de terre, grâce à une campagne nationale de collecte de données vectorielles en milieu urbain. En France, des groupes de travail se penchent sur le développement des JNT. Le programme Engineering Digital Twins (EDT) de l'Inria s'efforce de poser les bases scientifiques et technologiques nécessaires à la conception, la validation et l'évolution des jumeaux numériques. Le projet MINnD (Modélisation des INformations Interopérables pour les INfrastructures Durables) 2050[857], collaboratif depuis 2014, favorise l'intégration du BIM (Building Information Modelling) dans les infrastructures et anime un groupe de travail spécifique aux JNT, co-animé par des acteurs comme le Cerema, l'IGN, et la Métropole Européenne de Lille. De plus, en 2023, l'AFNOR a créé une commission nationale dédiée aux jumeaux numériques pour coordonner les initiatives françaises et influencer les travaux européens et internationaux en matière de normes sur le sujet [858].

Pour surmonter ces obstacles en matière de normalisation, plusieurs axes de recherche et de développement sont explorés. Les données satellites, par exemple, nécessitent des méthodes robustes d'alignement et de fusion 3D hétérogène. Cela inclut la détection et la sémantisation des changements, la régularisation vecteur, et de plus en plus, la classification des objets détectés via l'intelligence

---

853 Gaia-X est une initiative visant à développer une infrastructure de données fédérée et sécurisée pour l'Europe, dans laquelle les données sont partagées, les utilisateurs conservant le contrôle de l'accès à leurs données et de leur utilisation, et, selon certains, à assurer la souveraineté numérique de l'Europe. Elle vise à développer une gouvernance numérique basée sur les valeurs européennes de transparence, d'ouverture, de protection des données et de sécurité, qui peut être appliquée aux technologies en nuage pour obtenir la transparence et la contrôlabilité des données et des services. Source : https://gaia-x.eu/about/

854 Ávila Eça de Matos, B., Dane, G. Z., Van Tilburg, T., Verstappen, J., et de Vries, B., « State-of-the-Art of the Urban Digital Twin Ecosystem in the Netherlands », In M. Jalonen (Ed.), Smart Cities in Smart Regions 2022 Conference Proceedings, LAB University of Applied Sciences, pp. 37-53, 2022.

855 https://www.gov.uk/government/collections/the-national-digital-twin-programme-ndtp

856 https://www.mlit.go.jp/en/toshi/daisei/plateau_en_2.html

857 https://minnd2050.fr/

858 https://norminfo.afnor.org/structure/afnorcnjn/jumeaux-numeriques/212907

artificielle (IA). Ces techniques permettent une meilleure scalabilité et robustesse dans des environnements complexes. En parallèle, les modèles vectoriels en 3D, tels que ceux utilisant le formalisme CityGML[859] LOD2[860] à partir de données en nuage de points du LiDAR HD, ouvrent la voie à des référentiels multi-thématiques cohérents [861]. L'intégration des données repose aujourd'hui également sur les standards du web sémantique ou Web 3.0[862], comme Wikidata[863] ou DBpedia[864]. L'adoption de normes sémantiques internationales reconnues à travers la directive INSPIRE renforce également l'interopérabilité entre les jeux de données européens. Les graphes de connaissances et les outils comme Corese[865] ou Linkex[866] (développés par l'Inria) facilitent la découverte, l'alignement, et la

[859] La norme OGC Geographic Markup Language (GML), définit un codage XML conforme à la norme ISO 19118, pour le transport et le stockage d'informations géographiques modélisées conformément au cadre de modélisation conceptuelle utilisé dans la série de normes internationales ISO 19100 et incluant les propriétés spatiales et non spatiales des entités géographiques. Source : https://www.ogc.org/fr/publications/standard/gml/

[860] LOD2 (Level of Detail 2), désigne un niveau de détail intermédiaire dans la représentation des objets en 3D exploitant le langage GML.

[861] Lize Sanderson, « Point Cloud to 3D Terrain Model with Buildings », 2024. https://support.safe.com/hc/en-us/articles/25407508246413-Point-Cloud-to-3D-Terrain-Model-with-Buildings

[862] Le Web 3.0, également appelé web sémantique ou web des données liées, représente une évolution majeure du web en le transformant en une immense base de connaissances interconnectées. Contrairement au web des documents ou au web social (Web 2.0), il se concentre sur la structuration et l'exploitation intelligente des données, permettant des avancées significatives dans la recherche, la visualisation, la traduction et les raisonnements automatisés, bien au-delà des capacités des moteurs de recherche traditionnels. Bien qu'encore méconnu du grand public, son impact se manifeste principalement dans les couches profondes du web, souvent qualifiées de "web invisible", constituées des bases de données sous-jacentes. À terme, cette transformation influencera profondément le domaine culturel, en réorganisant les ressources numériques et en redéfinissant les outils et infrastructures numériques. Source : Ministère de la culture. Https://www.culture.gouv.fr/Thematiques/innovation-numerique/Faciliter-l-acces-aux-donnees-et-aux-contenus-culturels/Web-semantique-outils-pratiques

[863] Wikidata est une base de connaissances librement améliorable, conçue pour centraliser les données utilisées par les différents projets du mouvement Wikimédia. Une mise à jour d'une fiche Wikidata se répercute automatiquement sur toutes les pages de projets Wikimédia qui y font appel. Plus largement, Wikidata est destiné à fournir une source commune de données objectives, telles que les dates de naissance de personnalités ou le produit intérieur brut des pays. Source : Lausson Julien, « Wikidata veut faciliter la mise à jour de Wikipédia », Numerama, 31 mars 2012. https://www.numerama.com/tech/22208-wikidata-veut-faciliter-la-mise-a-jour-de-wikipedia.html

[864] DBpedia (de « DB » pour « database ») est un projet visant à extraire un contenu structuré des informations créées dans le cadre du projet Wikipedia. Ces informations structurées sont mises à disposition sur le World Wide Web à l'aide d'OpenLink Virtuoso. DBpedia permet aux utilisateurs d'interroger sémantiquement les relations et les propriétés des ressources de Wikipédia, y compris les liens vers d'autres ensembles de données connexes. Source : Bizer Christian, Lehmann Jens, Kobilarov Georgi, Auer Soren, Becker Christian, Cyganiak Richard et Hellmann, Sebastian, « DBpedia - A crystallization point for the Web of Data », Web Semantics : Science, Services and Agents on the World Wide Web, pp. 154–165, septembre 2009.

[865] Corese est une plateforme logicielle qui implémente et étend les standards du Web sémantique. Elle permet de créer, manipuler, analyser, sérialiser, interroger, raisonner et valider des données RDF. Source : Inria. https://project.inria.fr/corese/

[866] Linkex est un outil permettant de découvrir des clés de lien candidates à partir de deux ensembles de données RDF. Les clés de lien généralisent la combinaison des clés et des alignements d'ontologie pour l'interconnexion des données. Une clé de lien est un ensemble de paires de propriétés qui identifient de manière unique les instances de deux classes de deux ensembles de données RDF. Source : Abbas Nacira, David Jérôme, Napoli Amedeo, « Linkex: A Tool for Link Key Discovery Based on Pattern Structures », ICFCA 2019 - workshop on Applications and tools of formal concept analysis, Frankfurt, Germany. Pp. 33-38, juin 2019.

validation des données, tandis que les standards, tels que XML Schema[867] et JSON Schema[868] garantissent leur cohérence. Enfin, dans le domaine de l'IA, les travaux sur le GeoQuestionAnswering[869] visent à améliorer l'identification de données géographiques pertinentes pour appuyer des décisions précises dans des dispositifs d'aide à la décision aidés par intelligence artificielle. Enfin, en termes de visualisation et d'interaction, la recherche se concentre aujourd'hui sur des solutions immersives et collaboratives. Les interfaces actuelles, limitées à un usage mono-utilisateur sur postes fixes, évoluent vers des environnements multi-utilisateurs intégrant réalité augmentée (RA) et réalité virtuelle (RV). Ces techniques immersives associent perceptions digitales et contextes physiques, favorisant une interaction située, multisensorielle, et en temps réel. Le programme Engineering Digital Twins (EDT) de l'Inria s'inscrit dans ces efforts pour développer les fondements scientifiques et technologiques des JNT. Il explore des approches novatrices pour améliorer leur maintenance, leur évolution, et leur interaction avec des utilisateurs multisectoriels. Un autre défi central concernant le déploiement du JNFT est sa résilience aux attaques cyber. Destinée à accueillir un très grand nombre de données et de services, issues du privé comme du public, la sécurité du JNFT doit impérativement faire l'objet d'une surveillance particulière.

---

867 XSD (XML Schema Definition), une recommandation du World Wide Web Consortium (W3C), spécifie comment décrire formellement les éléments d'un document XML (Extensible Markup Language). Il peut être utilisé par les programmeurs pour vérifier chaque élément du contenu d'un document, afin de s'assurer qu'il adhère à la description de l'élément dans lequel il est placé. Source : Awati Rahul et Lawton Georges, « XML Schema Definition (XSD) », mai 2022. https://www.techtarget.com/whatis/definition/XSD-XML-Schema-Definition

868 JSON (JavaScript Object Notation) est un format de fichier et d'échange de données standard ouvert qui utilise du texte lisible par l'homme pour stocker et transmettre des objets de données constitués de paires nom-valeur et de tableaux (ou d'autres valeurs sérialisables). Il s'agit d'un format de données couramment utilisé pour divers usages dans l'échange de données électroniques, y compris celui des applications web avec les serveurs. Source : Ecma international, « ECMA-404 The JSON data interchange syntax », décembre 2017. https://ecma-international.org/publications-and-standards/standards/ecma-404/

869 Nous pouvons définir les questions géographiques comme des questions qui impliquent des entités géographiques (par exemple, Paris, France), des concepts géographiques (par exemple, des types d'entités tels que bâtiment, ville, État) ou des relations spatiales (par exemple, près de, au nord de, entre) en tant que parties des questions en langage naturel. Les systèmes d'IA ont encore du mal à comprendre précisément les questions entourant des données géographiques. GeoQuestionAnswering vise à résoudre ces problèmes et à faciliter la découverte et la compréhension des données géographiques par les intelligences artificielles. Source : Gengchen Maia, Krzysztof Janowicza, Rui Zhua, Ling Caia, et Ni Lao « Geographic Question Answering: Challenges, Uniqueness, Classification, and Future Directions », 24th AGILE Conference on Geographic Information Science, 2021. https://agile-giss.copernicus.org/articles/2/8/2021/agile-giss-2-8-2021.pdf

3.3 La nécessité de la cybersécurité dans le cadre du déploiement du Jumeau numérique des territoires

Les experts en cybersécurité ont étudié de longue date les risques cyber qui pèsent sur les jumeaux numériques [870]. Bien que les jumeaux numériques offrent des avantages significatifs en matière de simulation et d'optimisation, ils introduisent également de nouvelles surfaces d'attaque potentielle [871]. Il est donc crucial d'intégrer des mesures de sécurité dès la conception de ces systèmes et de rester vigilant face aux menaces émergentes. Les risques incluent les cyberattaques, les fuites de propriété intellectuelle, l'espionnage industriel et les accès non autorisés. Il est donc essentiel de mettre en place des mesures de sécurité robustes pour protéger ces systèmes. La sécurité des données manipulées par le JNFT est un défi central, particulièrement pour les données critiques issues des collectivités ou des industries stratégiques. La Géoplateforme, opérée par un consortium incluant Worldline[872] et Accenture[873] sur une infrastructure OVH[874], constituera le socle technologique et de sécurité sur lequel s'appuiera le Jumeau numérique de la France et des Territoires[875]. Déployée avec des outils avancés, cette plateforme met en œuvre de bonnes pratiques en matière de cybersécurité. Accenture, en partenariat avec l'IGN, a introduit des solutions éprouvées pour assurer une gestion efficace des incidents et le maintien en condition opérationnelle. Ces acquis devraient transférer au JNFT, notamment à travers l'approche DevSecOps[876], intégrant la sécurité à toutes les étapes du cycle de développement. Des audits réguliers et une surveillance renforcée seront à terme obligatoires afin de minimiser les risques d'attaques cyber, tout en répondant aux standards internationaux et européens.

---

870 K. Pratt Mary, « Les risques associés aux jumeaux numériques préoccupent les experts de la sécurité », CIO, 22 mai 2023. https://www.cio-online.com/actualites/lire-les-risques-associes-aux-jumeaux-numeriques-preoccupent-les-experts-de-la-securite-14942.html ?

871 Simpson Ilona, « The Security Implications of A Digital Twin », netskope, janvier 2024. https://www.netskope.com/fr/blog/the-security-implications-of-a-digital-twin ?

872 Worldline SA est une fintech (société financière) française fondée en 1972 et le numéro 4 mondial des sociétés de paiements. Worldline couvre l'ensemble de la chaîne de valeur des paiements en France et en Europe : traitement des émissions, acceptation des paiements, acquisition commerciale et traitement des acquisitions, ainsi que des services numériques complémentaires pour les administrations et les entreprises, au-delà des paiements. Source : https://worldline.com/fr-fr/home

873 Accenture plc est une société multinationale de services professionnels d'origine américaine dont le siège se trouve à Dublin, en Irlande. Elle est spécialisée dans les services de technologie de l'information (TI) et le conseil en gestion. Source : https://www.accenture.com/us-en/services/cybersecurity

874 OVH, légalement OVH Groupe SA, est une société française d'informatique en nuage qui propose des VPS (serveurs virtuels sécurisés), des serveurs dédiés et d'autres services web. Depuis janvier 2024, les offres hosted private cloud d'OVHCloud sont certifiées SecNumCloud 3.2 par l'ANSSI. Source : Dominique Filippone, « Après Outscale, OVH aussi certifié SecNumCloud 3.2 », Le Monde informatique, 9 janvier 2024. https://www.lemondeinformatique.fr/actualites/lire-apres-outscale-ovh-aussi-certifie-secnumcloud-32-92615.html

875 IGN, « L'IGN finalise son choix de partenaires techniques pour le développement et l'exploitation de la Géoplateforme », 27 janvier 2022. https://www.ign.fr/espace-presse/lign-finalise-son-choix-de-partenaires-techniques-pour-la-geoplateforme

876 Le DevSecOps est une méthodologie qui vise à inclure les pratiques de sécurité dans le processus de développement et de mise en production d'applications mis au point par l'ANSSI. Source : https://cyber.gouv.fr/publications/devsecops

Des mesures strictes seront à implémenter afin de garantir la protection des données et des systèmes. Comme évoqués dans le chapitre 5, les bases de données et les machines virtuelles (VM) sont des éléments critiques dans les infrastructures numériques modernes, en particulier pour des plateformes complexes, comme le Jumeau numérique de la France et des Territoires (JNFT). Leur protection nécessite des solutions antivirus robustes et adaptées aux spécificités de ces environnements. Dans le contexte du JNFT, où des volumes massifs de données sensibles sont traités et où la virtualisation est au cœur de l'architecture cloud, ces solutions de protection sont indispensables. L'antivirus agit comme une première ligne de défense contre les cyberattaques, renforçant la sécurité et la résilience de l'ensemble du système. Cependant, de simples antivirus ne suffiront pas à protéger une plateforme aussi large, d'autres solutions devront être développées, telles que l'inclusion d'un Web Application Firewall (WAF). Un WAF est une technologie de sécurité cruciale pour protéger les applications web contre diverses menaces en analysant et filtrant le trafic entrant et sortant. Contrairement aux pare-feu réseau classiques, qui protègent les couches réseau et transport, le WAF se concentre sur la couche applicative (niveau 7 du modèle OSI, cf. Figure 1), où la plupart des vulnérabilités critiques des applications web se manifestent[877]. Dans le cadre d'infrastructures comme le Jumeau numérique de la France et des Territoires (JNFT), où des volumes massifs de données sensibles sont manipulés, le rôle du WAF est capital. Il protège contre les cyberattaques visant à compromettre la disponibilité, l'intégrité ou la confidentialité des données géospatiales. Associé à d'autres mesures, comme l'analyse des journaux d'audit et la segmentation des accès, le WAF contribue à construire une plateforme résiliente et fiable.

Des mécanismes d'analyse automatique des vulnérabilités dans les déploiements de code devront également être mis en place. Ces analyses jouent un rôle central dans les environnements modernes où rapidité et sécurité sont essentielles, en particulier dans des systèmes complexes, comme les plateformes géospatiales ou les jumeaux numériques. Ces analyses permettent d'identifier et de corriger les failles avant qu'elles ne puissent être exploitées, renforçant ainsi la résilience des systèmes face aux cyberattaques. Dans les environnements DevSecOps, les analyses sont intégrées directement dans les pipelines d'intégration et de déploiement continus (Continuous Integration/Continuous Deployment). Chaque modification de code déclenche une série de tests de sécurité automatisés avant le déploiement en production. C'est cette approche, comme indiqué plus haut, qui devra être privilégiée pour la mise en place du JNFT. De plus, dans des projets massifs comme le Jumeau numérique de la France et des Territoires (JNFT), où de multiples services et modules sont déployés, ces analyses

[877] Endraca Alexander, King Bryan, Nodalo George, Sta Maricone, Sabas Maria et Isaac, « Web Application Firewall (WAF) », in *International Journal of e-Education, e-Business, e-Management and e-Learning*, Vol. 3, n° 6, décembre 2013. https://www.ijeeee.org/index.php?m=content&c=index&a=show&catid=41&id=595

permettent de sécuriser des volumes importants de code sans effort manuel excessif. Les analyses automatiques facilitent également la conformité aux standards en matière de cybersécurité (ISO 27001, RGPD) en générant des preuves de sécurité lors des audits.

Les données traitées par des systèmes critiques comme le JNFT doivent rester disponibles même en cas de panne ou d'attaque. La réplication quotidienne des données sur des sites séparés est une pratique clé pour répondre à cet enjeu. Les données devront être copiées en temps réel ou selon un calendrier défini vers plusieurs centres de données situés dans des régions distinctes. Cela réduira le risque de perte totale en cas d'incident localisé (incendie, panne électrique, cyberattaque). Toutes les données en transit ou au repos devront être chiffrées pour prévenir les interceptions ou altérations malveillantes. Des protocoles comme AES-256 sont généralement utilisés[878]. Un PRA (Plan de reprise d'Activité) devra également être défini. Un PRA est un ensemble de procédures conçues pour restaurer les systèmes et les données après un incident majeur[879]. Les tests réguliers de ce plan sont essentiels pour garantir son efficacité. Dans le cas du JNFT, ces pratiques sont particulièrement critiques en raison de la sensibilité des données géospatiales et de leur importance pour les collectivités et industries stratégiques. La combinaison de conteneurs sécurisés, de réplications géographiquement dispersées et d'un PRA rigoureusement testé garantit une plateforme résiliente face aux menaces modernes.

De plus, le JNFT sera adossé à la Géoplateforme nationale, lui permettant de profiter pleinement de la flexibilité offerte par cette dernière. Cette flexibilité repose sur l'intégration de technologies cloud standardisées, notamment Kubernetes[880], qui permet d'orchestrer des conteneurs pour des applications distribuées. Grâce à cette approche, le JNFT pourra facilement adapter ses capacités d'hébergement et de calcul pour répondre aux besoins croissants qui naîtront avec l'arrivée massive de données et les simulations complexes requises une fois le JNFT inauguré. Bien que le JNFT ne soit pas initialement déployé sur une infrastructure conforme à SecNumCloud, son architecture devra être pensée pour rester portable. Cela permettra une éventuelle migration vers des infrastructures restreintes à l'avenir, garantissant ainsi la gestion sécurisée de données critiques sans nécessiter de modifications structurelles majeures.

---

878 Advanced Encryption Standard ou AES (litt. « norme de chiffrement avancé »), aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique (aussi appelé « à clé secrète »). Il a été approuvé par la NSA (National Security Agency) dans sa Suite B des algorithmes cryptographiques. Source : https://luxsci.com/blog/256-bit-aes-encryption-for-ssl-and-tls-maximal-security.html

879 CNIL, « LA SÉCURITÉ DES DONNÉES PERSONNELLES », Le Guide de la CNIL, Ed. 2018, 2018, p. 20. https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_guide_securite_personnelle.pdf?

880 Kubernetes est un système open source qui vise à fournir une plateforme permettant d'automatiser le déploiement, la montée en charge et la mise en œuvre de conteneurs d'application sur des grappes de serveurs. Il fonctionne avec toute une série de technologies de conteneurisation, et est souvent utilisé avec Docker. Il a été conçu à l'origine par Google, puis offert à la Cloud Native Computing Foundation. Source : https://kubernetes.io/docs/concepts/overview/

Enfin, le déploiement opérationnel du JNFT s'appuiera sur des partenaires technologiques de pointe, tels qu'Eclairion[881] et Viridien[882], qui apporteront leur expertise respective en calcul haute performance (HPC) et en cloud souverain. Ainsi, Eclairion, reconnu comme un leader dans le domaine des supercalculateurs, mettra à disposition des infrastructures modulaires capables de traiter des charges de travail exigeantes en ressources. Ces infrastructures seront adaptées aux besoins spécifiques du JNFT, incluant : le traitement de données massives (big data), l'emploi d'algorithmes d'intelligence artificielle, la mise en place de simulations numériques intensives. De plus, le partenariat avec Eclairion garantira le stockage de l'ensemble des données sur le territoire national. Viridien, pour sa part, jouera un rôle clé dans l'optimisation des processus du JNFT grâce à son expertise en sciences des données et machine learning. L'objectif sera d'assurer un passage à l'échelle efficace des opérations, permettant au JNFT d'évoluer harmonieusement à chaque étape de son cycle de vie. Les technologies développées par Viridien faciliteront, l'analyse en temps réel des données, l'automatisation des processus et la collaboration entre les différents acteurs du projet grâce à des environnements partagés sécurisés. En adoptant une architecture modulaire et portable, le JNFT pourra s'intégrer facilement dans des infrastructures futures conformes à SecNumCloud. Cette anticipation est essentielle pour garantir la sécurité des données sensibles et répondre aux exigences des organismes publics et privés manipulant des informations critiques. L'utilisation de technologies ouvertes, comme Kubernetes, renforce cette portabilité, offrant une indépendance vis-à-vis des fournisseurs spécifiques et facilitant l'interopérabilité entre différentes plateformes cloud. Ainsi, cette approche repose sur une vision durable et innovante du traitement des données géographiques, où la flexibilité, la sécurité, et l'efficacité écologique se combinent pour soutenir des projets stratégiques à grande échelle.

Ainsi, le développement du Jumeau numérique de la France et des Territoires (JNFT) illustre une avancée technologique ambitieuse qui se doit d'allier innovation, sécurité et adaptabilité. Cette plateforme représente un enjeu stratégique majeur dans la gestion des données géographiques futures, dont l'importance pour les politiques publiques, les collectivités locales, et les industries stratégiques est indéniable. Toutefois, la protection cybernétique de ces infrastructures demandera des efforts coordonnés, un investissement financier important et une mise en œuvre rigoureuse des meilleures pratiques en matière de sécurité afin d'en garantir la pérennité.

---

[881] Eclairion est le premier centre de calcul en France dédié à l'hébergement en colocation de calculateurs haute densité dans des modules-conteneurs. Situé à Bruyères-le-Châtel, dans l'Essonne, ce centre offre une infrastructure souveraine, avec une capacité de 60 MW. Eclairion répond aux besoins croissants en matière de calcul intensif, notamment pour le Big Data, l'intelligence artificielle et la simulation numérique. Source : https://eclairion.com/

[882] Viridien, anciennement connue sous le nom de CGG, est une entreprise multinationale spécialisée dans les technologies de pointe, le digital et les données de la Terre. Viridien offre une expertise en sciences de la Terre, en analyse de données et en surveillance, proposant des solutions dans des domaines tels que l'imagerie du sous-sol, les services géologiques, les services numériques, ainsi que des solutions HPC et cloud. Source : https://www.viridiengroup.com/

Conclusion du chapitre VI

Comme démontré dans ce chapitre, les données géographiques numériques jouent un rôle essentiel dans le développement et la gestion des territoires, mais leur protection et leur exploitation posent de nombreux défis, notamment en raison du manque de moyens et de compétences spécialisées, particulièrement en cybersécurité. De plus, la diversité des bases de données et leur manque d'harmonisation compliquent leur exploitation. L'adoption de standards communs est essentielle pour garantir l'interopérabilité et l'efficacité des analyses territoriales. La gouvernance des données entre l'État et les collectivités est souvent unilatérale, avec une centralisation excessive des données par l'État et une redistribution tardive aux collectivités, freinant leur autonomie. De même, les décisions en matière de technologie prises au niveau national ne sont pas toujours adaptées aux réalités locales, créant des tensions et des inefficacités. Une situation exacerbée par le rôle plus important délégué aux régions dans la gestion des informations géographiques depuis le passage de la loi Notre. Alors même que l'État, attend plus d'autonomie et de participation des régions à la production de donnée, de nombreuses collectivités sont confrontés à un manque de moyen humain et financier important. Cette disparité creuse une inégalité territoriale marquée en matière de données géographiques, en particulier entre les métropoles, souvent très bien dotées et innovantes, et les espaces ruraux qui manquent de tout. Les initiatives du CNIG, en développant des normes reconnues par tous, et en offrant des espaces de partage entre les collectivités locales et les représentants de l'État, tendent à adoucir ces relations. Cependant ces initiatives ne suffisent pas totalement à régler l'ensemble de ces problèmes, et ne sont pas encore équipé pour faire face à certaines problématiques, notamment en matière de cybersécurité.

À l'heure de la généralisation des données ouvertes, de la transition numérique des services publics et de la démultiplication des capteurs géospatiaux, les territoires, qu'ils soient urbains ou ruraux, se trouvent confrontés à un ensemble de tensions nouvelles autour de la protection, de l'accessibilité et de la gouvernance de leurs données géographiques. Ce chapitre a mis en évidence les paradoxes croissants auxquels doivent faire face les collectivités territoriales, entre obligations de partage des données, dépendance technique à l'État central ou à des acteurs privés, et injonctions à renforcer leur autonomie numérique. La circulation des données géographiques s'inscrit dans des logiques de pouvoir multiscalaires, où s'entrecroisent enjeux de souveraineté, exigences d'interopérabilité, normes de cybersécurité et asymétries de ressources entre acteurs. Ce chapitre démontre que la protection des données géographiques ne saurait être réduite à une seule problématique technique ou juridique. Elle doit être pensée comme un processus géopolitique ancré dans l'espace, qui façonne les rapports de force entre institutions, entre niveaux de gouvernement, mais aussi entre modèles d'urbanisme, de gouvernance et de développement territorial. Ainsi, les difficultés rencontrées

par certaines collectivités à accéder en temps réel à leurs propres données, ou à celles qu'elles ont elles-mêmes contribué à produire, illustrent une forme de centralisation persistante qui entre parfois en contradiction avec les ambitions affichées de territorialisation des politiques publiques Les cas analysés, qui vont du retard dans la redistribution des données locales par l'État, aux frustrations liées à la conception centralisée des plateformes nationales telles que le Jumeau Numérique des Territoires, mettent en lumière des rivalités de légitimité et des conflits d'usages. Ils soulignent également la faible prise en compte, dans certains dispositifs nationaux, des besoins différenciés des territoires en matière de granularité, d'actualisation et de souveraineté des données. En retour, certains territoires développent leurs propres initiatives d'agrégation, de production ou de certification de données, ce qui participe à une reconfiguration des géographies de la gouvernance de l'information géographique.

L'absence de standards communs concernant l'ensemble des données entrave toujours l'interopérabilité des bases de données et limite leur potentiel analytique, tandis que certains acteurs, pour des raisons économiques ou politiques, restent réticents à partager leurs données. En parallèle, la montée en puissance des cyberattaques depuis 2020 fragilise les collectivités, notamment les plus petites, qui manquent de spécialistes en cybersécurité et peinent à recruter des experts en raison de grilles salariales peu attractives dans la fonction publique. Malgré une avancée significative dans l'ouverture des données publiques, des obstacles subsistent, notamment la fragmentation des plateformes de données et des problèmes d'interopérabilité. Certaines données sensibles (comme dans le monde agricole) ne sont pas toujours accessibles en raison de réticences politiques ou économiques. La rétention de données par certains acteurs freine l'exploitation de bases de données existantes. Les jumeaux numériques émergent comme des outils clé pour la gestion et la simulation des territoires grâce à des modèles 3D intégrant des données géographiques. Cependant, ces initiatives restent souvent isolées et non interopérables. Le projet national Jumeau Numérique de la France et des Territoires (JNFT), porté par l'IGN, le Cerema et l'Inria, vise à mutualiser ces initiatives à l'échelle nationale en fédérant collectivités et acteurs privés. Cependant, des enjeux de cybersécurité majeurs émergent, car ces plateformes traitent un grand volume de données sensibles. Ainsi, si le Jumeau Numérique des Territoires (JNFT) constitue une avancée majeure pour la transformation numérique des territoires, mais son succès dépendra de sa capacité à surmonter les défis liés à l'interopérabilité des données, à la cybersécurité et à la gouvernance multiacteurs. L'enjeu majeur est donc aujourd'hui d'assurer une collaboration efficace entre les collectivités, l'État et les entreprises privées, tout en garantissant la protection et l'accessibilité des données stratégiques à long terme.

En définitive, protéger les données géographiques numériques ne revient pas seulement à sécuriser leur accès ou à garantir leur intégrité. C'est aussi poser la question de qui gouverne les données, pour qui, et à quelles fins.

Conclusion de la partie 2

Cette deuxième partie avait pour ambition d'interroger la capacité des normes techniques à assurer la protection des données géographiques numériques, dans un contexte où le cyberespace apparaît de plus en plus structuré par des rapports de force géopolitiques. En articulant l'examen des enjeux généraux de la protection (chapitre IV), l'analyse des vulnérabilités propres aux infrastructures de données (chapitre V) et l'étude des défis territoriaux de la gouvernance (chapitre VI), cette partie a cherché à dégager les lignes de force d'une géopolitique de la donnée géographique numérique.

Il apparaît à l'issue de cette analyse que les données géographiques ne peuvent pas être appréhendées comme de simples objets techniques neutres. Elles constituent des ressources stratégiques dont la maîtrise engage directement la souveraineté des États et des territoires. Le conflit ukrainien a offert une démonstration révélatrice de cette mutation. Les attaques cyber dirigées contre des SIG en Ukraine ont révélé que l'information géographique numérique était devenue simultanément une arme et une cible. Cette dimension conflictuelle se retrouve à toutes les échelles, depuis l'intégration du cyberespace comme cinquième domaine de conflictualité par l'OTAN jusqu'à la multiplication des attaques visant les collectivités territoriales françaises, en passant par la création récente du Commissariat au numérique de défense. Ces évolutions témoignent d'une prise de conscience stratégique qui élève la protection des données géographiques au rang d'impératif de sécurité nationale.

L'analyse conduite révèle également une territorialisation paradoxale du cyberespace. Contrairement aux représentations courantes qui font de l'espace numérique un univers fluide et déterritorialisé, les dispositifs de gouvernance et de défense des données géographiques demeurent profondément ancrés dans des lieux précis. La localisation des centres d'excellence de l'OTAN, l'architecture institutionnelle française qui articule le CNIG, l'IGN, l'ANSSI et désormais le CND, ou encore la mosaïque des plateformes régionales d'information géographique dessinent une géographie singulière de la cybersécurité. Cette observation confirme que si les menaces circulent dans des réseaux déterritorialisés, les réponses institutionnelles et normatives restent, elles, gouvernées par des logiques territoriales qui engagent la souveraineté des États et l'autonomie des collectivités.

La normalisation occupe une place particulière dans ce dispositif. D'un côté, les standards de l'OGC et de l'ISO ont permis une interopérabilité sans précédent des systèmes d'information géographique, facilitant l'échange et le partage des données à l'échelle mondiale. De l'autre, cette ouverture a mécaniquement accru la surface d'attaque des infrastructures et complexifié leur sécurisation. L'émergence de normes spécifiques comme OGC WSS et GeoXACML traduit une prise

de conscience croissante de la nécessité d'intégrer les exigences de sécurité dès la conception des standards. Toutefois, l'examen des normes du DGIWG a montré que, dans le domaine militaire, l'impératif d'interopérabilité entre alliés continue de primer sur les considérations de cybersécurité. La normalisation apparaît ainsi comme un terrain de négociation géopolitique où s'affrontent des conceptions concurrentes de la sécurité, de l'ouverture et de la souveraineté.

Cette partie a par ailleurs cherché à mettre en lumière une géographie différenciée de la vulnérabilité cyber. L'exposition aux risques cyber n'est pas uniforme, elle varie selon les architectures techniques déployées, les moyens consacrés à la sécurisation et les compétences disponibles. Les asymétries entre les métropoles, généralement bien dotées en ressources numériques, et les territoires ruraux ou périphériques, qui peinent à recruter des spécialistes, dessinent une fracture numérique territoriale d'un genre nouveau. Les 218 incidents cyber recensés par l'ANSSI contre les collectivités territoriales en 2024 illustrent cette vulnérabilité structurelle que les dispositifs nationaux ne parviennent pas encore à résorber. Le rôle du CNIG comme arène de négociation a également révélé les rapports de pouvoir qui structurent la gouvernance des données géographiques, dans un contexte où la montée en puissance des GAFAM et le développement de communautés alternatives comme OpenStreetMap reconfigurent en permanence les équilibres établis. Sur le plan théorique, cette partie confirme la pertinence d'une approche géopolitique du cyberespace. Celui-ci n'abolit pas la géographie, mais la reconfigure. Les rivalités de pouvoir qui s'y déploient demeurent ancrées dans des territoires, portées par des acteurs situés et articulées à des représentations spatiales qui orientent les stratégies.

Plusieurs perspectives prolongent cette réflexion. L'évolution du cadre réglementaire européen, avec l'entrée en vigueur du Data Governance Act, du Data Act et de la directive NIS 2, impose de nouvelles obligations qui vont profondément remodeler le paysage de l'information géographique. Le projet de Jumeau numérique de la France et des Territoires cristallise également l'ensemble des tensions identifiées. Sa réussite dépendra de la capacité des acteurs à surmonter les défis de l'interopérabilité, de la cybersécurité et de la gouvernance multiacteurs. Enfin, la pénurie de spécialistes en cybersécurité, particulièrement aiguë dans les collectivités territoriales, constitue un obstacle majeur et sans montée en compétence généralisée, les ambitions affichées en matière de souveraineté numérique risquent de demeurer lettre morte.

En conclusion, il apparaît donc que la protection des données géographiques numériques ne saurait être réduite à une problématique technique ou juridique. Elle constitue un enjeu géopolitique à part entière, qui engage les rapports de pouvoir entre États, entre niveaux de gouvernement et entre acteurs publics et privés. La question transversale de cette thèse : qui gouverne les données, pour qui, et à quelles fins ? appelle des réponses qui dépassent le seul cadre technique pour engager des choix politiques fondamentaux sur la souveraineté, l'autonomie des territoires et les conditions de la

démocratie à l'ère numérique. Ces enjeux justifient un investissement renouvelé dans l'analyse des territorialités numériques émergentes pour la recherche en géographie, car protéger les données géographiques, c'est aussi préserver la capacité des sociétés à se représenter elles-mêmes et à maîtriser la connaissance de leurs territoires.

Partie 3 — Normalisation géospatiale et recompositions géopolitiques

La normalisation internationale, fondée sur des procédures de consensus entre une pluralité d'acteurs, est directement affectée par les recompositions géopolitiques contemporaines. L'intensification des rivalités et les ruptures diplomatiques entravent la production de compromis, elles fragilisent, ce faisant, l'efficacité d'un processus normatif devenu central depuis l'internationalisation accrue de l'économie à l'issue de la Seconde Guerre mondiale. Cette trajectoire n'a toutefois rien d'irréversible et des inflexions de politique publique, voire des orientations isolationnistes, peuvent réorienter les relations commerciales et reléguer la normalisation au second plan, jusqu'à la rendre ponctuellement inopérante.

Dans ce cadre, la dépendance des arènes de normalisation à la volonté des États et à leurs choix économiques se vérifie tout particulièrement pour les données géographiques. Le cas chinois illustre bien ces dynamiques. Longtemps peu impliquée dans les dispositifs internationaux, la République populaire de Chine s'est appuyée sur la profondeur de son marché intérieur avant d'opérer, au tournant des années 2000–2010, un retour volontariste porté par l'essor des technologies numériques. Cette réorientation s'est accompagnée d'une stratégie explicite d'influence, notamment à travers l'initiative « China Standards 2035 », perçue comme hégémonique par plusieurs pays, en particulier en Occident. Elle peut néanmoins être lue, du point de vue de la structuration des échanges, comme un mouvement de normalisation d'une situation antérieure atypique : une plus grande intégration de l'économie chinoise via des normes partagées est susceptible d'améliorer l'accessibilité et la prévisibilité de ce marché pour l'ensemble des acteurs.

Parallèlement, l'évolution de la posture américaine et les reconfigurations d'alliances qu'elle induit interrogent la stabilité de l'ordre normatif international. Les inflexions protectionnistes, les tensions commerciales et la redéfinition de priorités stratégiques affectent l'équilibre des contributions d'experts et la capacité des instances internationales à produire des standards universellement acceptés. L'ensemble de ces éléments éclaire la problématique qui guide cette partie : comment les recompositions de puissance et les transformations technologiques reconfigurent-elles la capacité à produire des normes géospatiales interopérables, et selon quelles stratégies d'acteurs (États, organisations, entreprises) l'Europe, et la France en son sein, peuvent-elles maintenir ou renforcer leur influence normative ?

La troisième partie de cette thèse s'organise en trois volets complémentaires. Le chapitre VII, consacré à la recomposition géopolitique et au processus normatif, analyse d'abord la manière dont les rivalités contemporaines reconfigurent la standardisation, en portant une attention particulière à la position singulière de l'Union européenne et aux conditions d'un renforcement de son influence. Il examine ensuite l'essor des espaces communs de données destinés à consolider l'interopérabilité au-delà des frontières nationales, tout en soulignant la persistance de fractures dans la gouvernance mondiale des normes.

Le chapitre VIII, centré sur le poids des technologies émergentes, évalue l'impact de l'intelligence artificielle, de la blockchain, des jumeaux numériques et des environnements immersifs sur les référentiels techniques. Il met en évidence les exigences inédites que ces innovations imposent en matière d'interopérabilité, ainsi que les enjeux associés de cybersécurité, notamment dans la perspective post-quantique. L'analyse articule, enfin, les promesses d'innovation et les vulnérabilités nouvelles qu'elles introduisent au sein des infrastructures géospatiales.

Enfin, le chapitre IX, orienté vers la prospective et les scénarios d'évolution, propose trois trajectoires contrastées. En premier lieu l'hypothèse de la fragmentation en blocs, puis celle de la convergence multiacteurs, et enfin celle d'une possible domination de standards privés de facto, et discute les stratégies d'influence qui leur correspondent, depuis les registres diplomatiques étatiques jusqu'aux coalitions industrielles. Enfin, une attention particulière est donnée aux implications pour la normalisation de défense, en analysant le rôle respectif de l'OTAN et de l'Union européenne, l'avenir des programmes de coproduction géospatiale, et les modalités d'articulation entre acteurs publics et privés.

Comme souligné dans les parties précédentes, la normalisation internationale est directement concernée par les bouleversements géopolitiques qui affectent le monde entier. La normalisation internationale se fait souvent le reflet des tensions internationales. Le modèle international de normalisation étant fondé sur le consensus d'acteurs divers, l'accroissement des tensions entre différents pays a souvent un impact direct sur l'efficacité du processus normatif. Le dialogue et le compromis étant les « armes » de la normalisation, en cas de rupture diplomatique, ce processus se retrouve largement empêché. L'internationalisation de l'économie mondiale depuis la fin de la Seconde Guerre mondiale a largement contribué à l'émergence de la normalisation internationale comme composante clé du commerce mondial. Cependant, cette réalité n'est pas gravée dans le marbre. Les changements de politique peuvent directement impacter les relations commerciales, et faire de la normalisation une priorité secondaire, voire la rendre impossible. Les stratégies isolationnistes prônées par certains États sont des obstacles à leur intégration dans l'économie mondiale, et les instances normatives internationales. Comme indiqué dans la première partie de cette thèse, la République

Populaire de Chine fait office de cas d'école en la matière. Cette dernière s'étant presque totalement désintéressée de la normalisation internationale pendant des décennies, s'appuyant sur son marché interne pour bâtir son empire industriel, avant d'y faire un retour fracassant dans les années 2000 – 2010 à l'aune de sa recherche de diversification économique, notamment en direction des nouvelles technologies.

Ainsi, les processus de normalisation internationaux ne sont pas épargnés par les logiques d'influence et d'alliance, que ce soit dans les accords entre États ou entre firmes. En réalité, ils sont très dépendants du bon vouloir des États et de leur politique économique. Cela vaut aussi pour la normalisation des données géographiques. Aujourd'hui, la Chine donne l'exemple d'une poussée intégratrice de la deuxième économie mondiale, au sein du système international de normalisation, qui fait plus office de correction d'une situation antérieure tenant de l'anomalie qu'autre chose. Ce regain d'intérêt de la Chine pour la normalisation internationale s'est accompagné d'une politique volontariste et d'une véritable volonté de domination des instances internationales, comme l'a bien souligné le projet « China Standards 2035 ». Cette nouvelle politique a suscité des remous dans plusieurs pays, notamment en Occident, en raison de la volonté manifeste de domination. Cela étant dit, une plus grande intégration de l'économie chinoise dans l'économie mondiale, par le biais des normes internationales, constitue une évolution positive par rapport à la situation antérieure, qui rendait difficilement accessible le premier marché mondial en termes de consommateurs.

Au même moment, la position des États-Unis, qui représentent la première économie mondiale, concernant la normalisation internationale, apparaît plus alarmante. Alors que le nombre d'experts américains ne fait que baisser depuis 2015, la réélection de Donald Trump à la tête du pays fait peser un risque très important pour la normalisation internationale. La volonté isolationniste du président Trump, ainsi que le déploiement de tarifs « réciproques » contre l'ensemble des pays du monde (à l'exception notable de la Russie), va provoquer un véritable séisme économique, mais aussi politique dans le monde entier[883]. Pour la normalisation internationale, un retrait des États-Unis pourrait provoquer d'importants dysfonctionnements pour de nombreux pays, notamment en Europe. Ces derniers verraient des stratégies économiques élaborés de longue date être mis à mal. De plus, dans le chaos qui s'ensuivrait, il y a fort à parier que la Chine serait en position de force pour renforcer son influence au sein des instances de normalisation internationales. Les changements concernant la diplomatie américaine, et la volonté affichée de l'actuel président de s'aliéner ses principaux alliés, en Europe comme en Amérique du Nord, ouvrent la voie à une période extrêmement incertaine en matière de relation internationale, diplomatiquement comme économiquement.

[883] Tax Foundation, « Trump Tariffs: Tracking the Economic Impact of the Trump Trade War », 3 avril 2025. Consulté le 4 avril 2025. https://taxfoundation.org/research/all/federal/trump-tariffs-trade-war/

Chapitre VII – Recomposition géopolitique et processus normatif : quel avenir pour la France et l'Europe ?

Alors que la guerre en Ukraine se poursuit, l'hostilité américaine fait craindre un retrait militaire pur et simple des États-Unis d'Europe, voire un abandon de l'OTAN. Une telle situation aurait de graves conséquences pour la défense européenne, et pourrait remettre en question toutes les logiques d'interopérabilité qui sous-tendent actuellement le développement des programmes de normalisation militaires européens, en matière de données géographiques comme ailleurs. Le redécoupage de l'ancien équilibre hérité de la guerre froide auquel nous assistons aujourd'hui fait naître un grand nombre de défis pour la France et les nations européennes dans leur ensemble. Cette incertitude entraîne également avec elle un monde d'opportunités à saisir pour l'Europe, reste cependant à voir si une réponse cohérente pourra être mise sur pied afin de répondre à ces nouveaux défis. En matière de normalisation, les enjeux sont également grands, du fait notamment du fonctionnement même des instances internationales de normalisation. Les jeux d'influence continuent de se jouer au sein de ces instances, et l'élaboration d'une stratégie cohérente en matière de normalisation doit continuer à être une priorité pour la France si elle veut espérer pouvoir continuer à jouer un rôle important. La redéfinition des relations internationales va probablement entraîner avec elle une refondation des alliances traditionnelles, de nouveaux partenaires émergent et vont chercher à occuper l'espace laissé vacant par les États-Unis. Si la Chine fait figure de candidat évident pour la reprise du leadership mondial, dans le domaine de la normalisation comme ailleurs, il ne faut pas écarter non plus que d'autres partenaires en Asie et en Amérique vont également tirer leurs propres conclusions de ces développements et adapter leur stratégie en conséquence.

1. La recomposition géopolitique rebat les cartes de la standardisation internationale

Alors que la guerre en Ukraine entre dans son quatrième été, Kyiv et ses partenaires doivent mettre à l'épreuve leur détermination, leur état de préparation et leur engagement en faveur de la sécurité européenne. Pour la première fois depuis plus d'un demi-siècle, le gouvernement suédois a publié des brochures d'information publique indiquant aux ménages ce qu'ils doivent faire en cas de guerre [884]. Dans le même temps, les récents barrages de missiles russes visant l'infrastructure énergétique de l'Ukraine ont déjà privé des millions de personnes d'électricité [885]. Alors même que l'Alliance entre les États-Unis et l'Europe, qui semblait définir le monde occidental, semble toucher à sa fin [886], c'est toutes les stratégies, diplomatiques, économiques et militaires qui doivent aujourd'hui être repensées face à cette véritable recomposition géopolitique. La recomposition géopolitique désigne ici un processus de réagencement durable des rapports de puissance entre acteurs étatiques et non étatiques, se traduisant par des modifications multiéchelles des alliances, des institutions, des régimes normatifs et des territorialités des flux. Elle implique des changements structurels, qui renégocient les hiérarchies entre le centre et la périphérie et redessinent les espaces d'influence[887]. Cette remarque est valable pour l'ensemble des pays membres de l'Union européenne.

La possibilité d'un morcellement de l'environnement normatif international est aujourd'hui une hypothèse qui doit être prise très au sérieux. Face à ces difficultés, il semble aujourd'hui nécessaire de réfléchir à ces problématiques en matière d'oppositions multipolaires, où différents blocs, à la fois normatifs, militaires et diplomatiques, pourraient être amenés à se construire, là où se trouvait autrefois le leadership américain. La France a de nombreux atouts à exploiter. Cependant, les réponses à ces problèmes émergents doivent être abordées à l'échelle de l'Union européenne, où les stratégies et solutions doivent être élaborées. C'est en effet, par le biais du poids économique et diplomatique offert par une Europe unie face à ces enjeux, que des solutions efficaces pourront être mises en place. De plus, l'Europe demeure un poids lourd de la normalisation internationale, coordonnant les normes du

---

884 Associated Press News, « Sweden updates its Cold War-era preparedness booklet », 8 octobre 2024. https://apnews.com/article/sweden-booklet-disaster-cold-war-8becf7aa9aa9cd1f8eb522343e163bdd. Consulté le 1er décembre 2024.

885 Novikov Illia, « Russia targets Ukrainian energy infrastructure with massive cruise missile and drone attack », Associated Press News, in PBS News, 13 décembre 2024. https://www.pbs.org/newshour/world/russia-targets-ukrainian-energy-infrastructure-with-massive-cruise-missile-and-drone-attack. Consulté le 2 janvier 2025.

886 Rhode Benjamin, « Europe Without America », Survival, 66(2), 2024, pp. 7–18. https://doi.org/10.1080/00396338.2024.2332054. Consulté le 2 avril 2025.

887 John Agnew, « The Territorial Trap: The Geographical Assumptions of International Relations Theory », in *Review of International Political Economy*, Vol 1 (1), Spring, 1994, pp. 53-80.

plus grand marché unique mondial. Elle doit prendre toute la mesure de sa puissance afin de s'appuyer sur elle de façon adéquate. Le poids économique de l'Europe est son premier atout, et c'est uniquement à travers une coopération accrue avec ses alliés européens que la France pourra pleinement faire jouer ses atouts et faire face à l'avenir incertain qui se présente à elle.

1.1. Le renouvellement du rôle de l'Union européenne comme agent structurant des luttes de pouvoir en matière de standardisation internationale

La normalisation européenne s'inscrit dans un contexte mondial de plus en plus concurrentiel. Dans sa stratégie en matière de normalisation publiée en février 2022, la Commission européenne constate que *« de nombreux pays tiers adoptent une position ferme en matière de normalisation, offrant à leurs industries un avantage concurrentiel pour ce qui est de l'accès au marché et du déploiement des technologies »*[888]. Elle en déduit que la compétitivité et la souveraineté technologique de l'Europe dépendront du succès de ses acteurs dans la normalisation internationale, ce qui suppose de solides compétences dans l'industrie et le monde universitaire, ainsi qu'une normalisation européenne plus souple, plus rapide et mieux ciblée. En effet, la Commission reconnaît que des consortiums souvent privés, piloté par des industriels de pays tiers, sont plus rapide dans l'élaboration de normes, et que, concernant les nouvelles technologies, le système européen *« est souvent incapable de fournir ses produits en temps utile et perd donc l'important « avantage du précurseur » qu'offre la normalisation »*. Le domaine des technologies de l'information, dont relève la géographie numérique est directement concerné.

Par conséquent, outre les travaux de normalisation en cours dans les écosystèmes industriels, la Commission européenne considère que l'Union européenne est aujourd'hui confrontée à des « urgences de normalisation » critiques, des domaines dans lesquels des normes sont nécessaires dans les années à venir afin d'éviter les dépendances stratégiques et de manifester la position de leader mondial de l'UE dans le domaine des technologies numériques. Il s'agit notamment des normes de certification des puces en termes de sécurité, d'authenticité et de fiabilité, et des normes concernant les données qui améliorent l'interopérabilité, le partage et la réutilisation des données à l'appui de l'espace européen commun de données[889]. Ainsi, il est possible de dégager une série d'écueils frappant la normalisation européenne. Parmi ceux-ci, on compte le manque de formation aux enjeux de la normalisation internationale dans l'éducation supérieure des différents pays européens, le manque de financement

[888] Commission européenne, Communication au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Une stratégie de l'UE en matière de normalisation. Définir des normes mondiales à l'appui d'un marché unique européen, vert et numérique », COM(2022) 31 final, Bruxelles, 2 février 2022, p.1.

[889] Ibid

accordé aux activités de la standardisation internationale, un besoin accru en matière d'interopérabilité des données, ainsi qu'un manque d'alignement entre les normes européennes et internationales.

Depuis plus de trois décennies, l'Union européenne joue un rôle central dans l'élaboration des normes, y compris sur la scène internationale, affirmant ainsi son leadership technologique, comme l'a rappelé le rapport final du chantier n°4 du Forum de haut niveau sur la normalisation européenne (HLF)[890]. Selon ce rapport, cette influence a permis d'éviter la prolifération de variantes régionales des normes internationales en Europe, favorisant ainsi un alignement cohérent entre les référentiels européens et internationaux. Cet alignement a constitué un atout majeur pour la compétitivité mondiale des entreprises européennes, leur garantissant un accès facilité aux marchés internationaux. Les Accords de Vienne[891] et de Francfort[892] ont joué un rôle clé dans ce processus en établissant un principe fondamental qui est la primauté des normes internationales sur les standards nationaux et régionaux. Cette approche a permis de renforcer la cohésion entre les cadres normatifs européens et internationaux, facilitant ainsi l'adoption de références techniques communes à l'échelle mondiale. Cependant, ces dernières années, l'essor des révolutions numériques, notamment dans les domaines des semi-conducteurs, de l'informatique personnelle, du Web, de la communication mobile et de l'intelligence artificielle, a profondément modifié le paysage de la normalisation. Parallèlement, la montée en puissance économique et technologique de plusieurs pays en développement, combinée aux évolutions du contexte géopolitique, a conduit un nombre croissant d'experts issus de ces pays à intégrer les comités internationaux de normalisation[893]. Cette dynamique a intensifié la compétition stratégique au sein des instances normatives, certains acteurs cherchant activement à influencer les processus décisionnels en fonction de leurs propres intérêts industriels et technologiques. Dans ce contexte, il peut en résulter des dissensions sur l'adéquation des normes internationales aux besoins spécifiques du marché européen. La capacité de l'UE à maintenir son influence et à garantir que les normes internationales continuent de soutenir son modèle économique et technologique repose désormais sur sa capacité à s'adapter à ces nouveaux enjeux et à défendre ses positions stratégiques au sein des instances de normalisation mondiales.

---

890 Hihg Level Forum on European Standardisation, « Alignment between Europen and International Standards », rapport final du chantier n°4 (pilote : Orgalim), Ares (2025)288593, 15 janvier 2025, p.2.

891 ISO & CEN, « Lignes directrices relatives à la mise en œuvre de l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne) », (7), 2016. https://boss.cen.eu/media/CEN/ref/va_guidelines_implementation_fr.pdf. Consulté le 25 avril 2022.

892 CENELEC, « GUIDE 13 IEC - CENELEC Agreement on Common planning of new work and parallel voting », (3), octobre 2016. https://www.cencenelec.eu/media/Guides/CLC/13_cenelecguide13.pdf. Consulté le 2 mars 2022.

893 L'Organisation internationale de normalisation (ISO) souligne que plus des trois quarts de ses membres proviennent de pays en développement, ce qui témoigne de leur engagement croissant dans l'élaboration des normes internationales. https://www.iso.org/who-develops-standards.html

Comme le détaille le rapport du chantier n°4 du HLF, l'élaboration des normes harmonisées repose sur une demande de normalisation formulée par la Commission européenne[894]. La demande de normalisation de la Commission européenne (en anglais Standardisation Request (SR)), anciennement appelée mandat de normalisation, qui est adressée aux organismes européens de normalisation (CEN, CENELEC, ETSI), est généralement formalisée sur le fondement de l'art. 10 du règlement (UE) n° 1025/2012 (souvent via une décision d'exécution)[895]. Ce document, rédigé par la Commission, fait l'objet d'un processus de consultation et de discussion approfondie impliquant les Organismes européens de Normalisation (OEN), ainsi que d'autres parties prenantes concernées et experts sectoriels des États membres. Une fois validée et acceptée par les OEN, la demande est ensuite transmise aux comités techniques (CT) compétents, déjà engagés dans l'élaboration de normes répondant aux besoins du marché dans le domaine concerné. Dans certains cas, un nouveau comité technique ou un groupe de travail affilié à un comité existant peut être créé afin de mener à bien cette mission. Concernant les normes européennes harmonisées (hEN) développées par le CEN[896] et le CENELEC[897], elles peuvent être alignées sur les normes internationales selon deux approches distinctes. Quel que soit le mode d'élaboration retenu, une fois finalisées, les normes demandées par la Commission européenne doivent faire l'objet d'une évaluation rigoureuse pour vérifier leur conformité aux exigences législatives en vigueur. Cette validation est une étape clé permettant leur référence dans le Journal Officiel de l'Union européenne, leur conférant ainsi une présomption de conformité avec la réglementation. Lorsque les normes sont élaborées au niveau international par l'ISO, elles peuvent être adoptées en tant que normes européennes par le CEN et le CENELEC à travers les Accords de Vienne et de Francfort. Ces normes peuvent être reprises telles quelles ou faire l'objet d'amendements spécifiques, avant d'être référencées au Journal Officiel de l'Union. Dans les processus internationaux de normalisation basés sur le consensus, le secrétariat du comité technique en charge des travaux peut être dirigé aussi bien par un organisme de normalisation européen que par un organisme national d'un pays tiers. Lorsqu'une approche nationale est privilégiée, le CEN et le CENELEC élaborent la norme directement. Dans ce cas, il peut exister ou non une norme internationale traitant d'exigences similaires. Si des normes internationales pertinentes sont disponibles, elles peuvent servir de référence

---

894 Hihg Level Forum on European Standardisation, « Alignment between Europen and International Standards », rapport final du chantier n°4 (pilote : Orgalim), Ares (2025)288593, 15 janvier 2025, p.2.

895 Règlement (UE) N°1025/2012 du Parlement européen et du Conseil, du 25 octobre 2012, relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision no 1673/2006/CE du Parlement européen et du Conseil. Disponible ici : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025. Consulté le 15 novembre 2025.

896 Comité européen de normalisation

897 Comité européen de normalisation pour l'électrotechnique.

ou être intégrées partiellement dans la norme européenne. En revanche, si aucune norme internationale équivalente n'existe, une norme développée au niveau national peut, si elle s'avère pertinente à une échelle mondiale, être adoptée ultérieurement comme référence internationale. Cette dynamique permet ainsi d'assurer une cohérence globale et d'éviter des divergences inutiles entre les cadres normatifs européens et internationaux.

Ce même rapport souligne que les normes européennes harmonisées (hEN) développées par l'ETSI[898] suivent une procédure distincte en ce qui concerne leur adoption à l'échelle internationale[899]. Contrairement aux normes élaborées par le CEN et le CENELEC, qui peuvent être intégrées au cadre international via les accords de Vienne et de Francfort, l'ETSI ne bénéficie pas d'un équivalent institutionnel reconnu au niveau mondial, tel que l'ISO ou la CEI, auprès desquelles il pourrait soumettre ses normes pour adoption ou obtenir une reconnaissance officielle de ses travaux à l'international. Ainsi, les normes élaborées au sein des comités techniques de l'ETSI sont spécifiquement destinées au secteur des technologies de l'information et de la communication. Bien que ces normes soient développées dans un cadre européen, un grand nombre d'entre elles, qu'elles soient harmonisées ou non, trouvent une application au-delà des frontières de l'UE. Cette diffusion internationale s'explique en partie par le système d'adhésion ouvert mis en place par l'ETSI, qui permet à des acteurs publics et privés du monde entier de participer directement aux travaux de normalisation. Grâce à cette approche collaborative, de nombreuses normes issues de l'ETSI possèdent une portée internationale dès leur conception. En parallèle, l'ETSI s'est associé à d'autres Organismes internationaux de Normalisation pour créer le projet de partenariat de troisième génération (3GPP)[900]. Cette initiative vise à développer des spécifications techniques pour les systèmes cellulaires, qui sont ensuite transposées au niveau régional par les OEN participants. De plus, ces spécifications bénéficient d'une reconnaissance mondiale grâce à leur adoption par l'Union Internationale des Télécommunications, qui les recommande comme références techniques dans le cadre de la normalisation des réseaux mobiles à l'échelle planétaire.

Le rapport du HLF identifie également plusieurs avantages à l'alignement entre normes européennes et internationales. Le premier réside dans l'assurance de la compatibilité, permettant aux produits d'être interchangeables sur les marchés mondiaux. Cette interopérabilité est particulièrement cruciale dans les chaînes d'approvisionnement globales, où les différents fournisseurs peuvent se

---

898 Institut européen des normes de télécommunications

899 Hihg Level Forum on European Standardisation, « Alignment between Europen and International Standards », rapport final du chantier n°4 (pilote : Orgalim), Ares (2025)288593, 15 janvier 2025, p.2.

900 3rd Generation Partnership Project (3GPP) est une coopération entre organismes de normalisation en télécommunications tels que : l'UIT (union internationale des télécommunications), l'ETSI (Europe), l'ARIB/TTC (Japon), le CCSA (Chine), l'ATIS (Amérique du Nord) et le TTA (Corée du Sud). Il produit et publie les spécifications techniques pour les réseaux mobiles de 3e (3G), 4e (4G) et 5e (5G) générations. Source : https://www.3gpp.org/about-us.

spécialiser dans des composants spécifiques tout en respectant une référence commune. En adhérant aux mêmes normes, ils peuvent ainsi s'intégrer efficacement dans la production de biens complexes, favorisant une meilleure répartition des expertises et une optimisation de la spécialisation industrielle. Au-delà de cet aspect, les normes jouent également un rôle déterminant dans la stimulation de l'innovation. En fournissant un cadre technique structuré, elles encouragent le développement de nouvelles technologies tout en assurant une cohérence réglementaire entre les différents acteurs du marché. De plus, l'adoption de normes internationales facilite l'accès aux marchés étrangers, tout en réduisant les charges administratives et les coûts de mise en conformité pour les entreprises. Au contraire, lorsque plusieurs normes coexistent dans différentes régions, cela peut compliquer la conception des produits et rendre leur homologation plus laborieuse. Les divergences normatives peuvent entraîner des contraintes significatives pour les fabricants. Une entreprise confrontée à des exigences disparates selon les régions peut être obligée d'adapter la conception de ses produits, voire de mettre en place des chaînes de production distinctes pour répondre aux spécificités de chaque marché. De surcroît, le besoin de réaliser des tests multiples et de gérer une documentation technique variée pour un même produit alourdit les processus et entraîne des coûts supplémentaires. Ces obstacles peuvent retarder la mise sur le marché, accroître les dépenses de production et nuire à la compétitivité globale des entreprises concernées.

Pour autant, le même rapport reconnaît que l'alignement systématique des normes européennes sur les normes internationales n'est pas sans risques ni limites[901]. Les normes européennes dites harmonisées jouent un rôle particulier dans le cadre juridique de l'Union : lorsqu'elles sont citées au Journal Officiel, elles confèrent une présomption de conformité vis-à-vis des exigences des directives et règlements européens en vigueur. Un alignement trop strict sur une norme internationale pourrait donc s'avérer inapproprié si cette dernière ne reflète pas pleinement les spécificités du marché européen ou les valeurs sociétales de l'UE. Par exemple, l'Union attache une importance singulière à la protection des données personnelles (y compris géolocalisées) et à des principes éthiques dans l'utilisation des technologies, qui peuvent dépasser les standards minimalistes admis ailleurs. De même, certaines exigences réglementaires européennes, liées par exemple à la sécurité des infrastructures critiques ou à la qualité des données environnementales, peuvent justifier l'existence de normes propres à l'UE plus strictes que l'équivalent international. Dans ces cas, une non-équivalence maîtrisée entre les normes européennes et internationales est parfois nécessaire pour préserver les intérêts stratégiques de l'Union. L'objectif n'est pas de verser dans un isolationnisme normatif, mais de garantir que là où c'est justifié, l'Europe maintienne des exigences techniques élevées en phase avec

[901] Hihg Level Forum on European Standardisation, « Greater inclusiveness of civil society and SMEs in international standardisation », rapport final du chantier n°5 (pilote : Orgalim), Ares (2025)288593, 15 janvier 2025, p.9.

ses priorités, par exemple en matière de durabilité, d'accessibilité ou de souveraineté numérique. Une telle divergence contrôlée peut impliquer d'adapter une norme ISO lors de son adoption en Europe, ou à l'extrême, de développer provisoirement une norme européenne en l'absence de consensus mondial satisfaisant. Naturellement, ces situations doivent rester l'exception afin de ne pas compromettre l'unité du marché mondial : l'idéal recherché demeure une convergence maximale, où les normes internationales intègrent en amont les préoccupations européennes plutôt que d'obliger l'UE à s'en écarter a posteriori.

Le rapport du HLF souligne également qu'il demeure cependant difficile d'évaluer avec précision le degré de divergence entre normes internationales et normes européennes, notamment dans le champ géospatial, faute d'un système structuré de collecte de données à l'échelle de l'UE sur ce sujet[902]. Le suivi de la couverture normative, c'est-à-dire le taux d'équivalence entre les référentiels, est encore lacunaire. Mettre en place un tel dispositif de suivi permettrait de mesurer rigoureusement le délai écoulé entre la publication d'une norme à l'ISO, son adoption formelle comme norme européenne, puis, pour les normes harmonisées, sa citation au Journal Officiel de l'Union. Si certaines données existent déjà, ces trois étapes ne sont pas systématiquement corrélées dans les rapports actuels, ce qui limite les analyses. Au-delà des délais, il serait crucial d'identifier les facteurs influençant les écarts d'adoption afin de comprendre les causes des retards ou des non-alignements. Plusieurs paramètres peuvent être envisagés : la nationalité de l'organisme secrétaire du comité technique international, la répartition géographique des experts dans ce comité, ou encore l'existence d'un comité européen miroir actif en parallèle pour préparer la transposition. Par exemple, la présence d'un comité miroir CEN pour l'ISO/TC 211 (information géographique) a sans doute facilité l'adoption rapide en Europe de nombreuses normes ISO 191xx. Inversement, l'absence de comité miroir européen sur un sujet donné peut laisser un vide et retarder la diffusion du standard international au sein de l'UE. Le temps de transposition au CEN/CENELEC est un autre indicateur clé. En effet, certaines normes ISO, une fois publiées, mettent plusieurs années avant d'être disponibles en tant que normes EN, selon la complexité du sujet et la charge de travail des commissions nationales. Enfin, il convient de suivre la gestion du cycle de vie des normes. Le délai avant le retrait des anciennes versions de normes européennes peut influencer la vitesse d'adoption des nouvelles versions par les acteurs économiques. Il arrive aussi qu'une norme européenne n'ait pas d'équivalent international du tout, c'est le cas de certaines spécifications développées pour INSPIRE ou de standards élaborés dans un contexte de défense européenne. Dans certaines situations, ces normes « locales » pertinentes peuvent être proposées à la suite de l'ISO ou à l'OGC pour en faire des références mondiales, comme ce fut le cas

[902] Hihg Level Forum on European Standardisation, « Alignment between Europen and International Standards », rapport final du chantier n°4 (pilote : Orgalim), Ares (2025)288593, 15 janvier 2025, p.16

par exemple du modèle de données européen pour l'occupation des sols Corine Land Cover, repris dans des travaux internationaux.

D'où l'importance de suivre les taux d'adoption et les délais associés, tant dans le sens international → Europe que dans le sens Europe → international. Un cadre de collecte de données bien conçu devrait ainsi permettre d'identifier la part de normes européennes acceptées ou non au niveau mondial, et vice-versa, en isolant les retards éventuels. Afin d'assurer la comparabilité des informations recueillies, un accord méthodologique clair entre les organismes de normalisation serait nécessaire, de sorte que chaque État et chaque OEN remonte les données de manière homogène. D'où l'importance de disposer de ces indicateurs, qui constitueraient un outil précieux pour la Commission européenne et les parties prenantes, en éclairant les décisions stratégiques : par exemple, détecter qu'un standard géospatial met systématiquement plus de 3 ans à être adopté en Europe pourrait conduire à renforcer la participation des experts européens dans le comité ISO concerné, ou à initier plus tôt la création d'un comité miroir pour gagner du temps.

Le rapport recommande également que le CEN et le CENELEC identifient, sur la base du jugement des experts des comités techniques, les modifications de normes internationales qui entraînent un découpage partiel et qui suivent les nouvelles versions non encore adoptées en Europe[903]. Autrement dit, il s'agit de surveiller si les évolutions des normes internationales, notamment dans le numérique et la géospatiale, introduisent des éléments incompatibles avec les exigences ou préférences européennes, ce qui aboutirait à un découplage partiel des référentiels. Pour assurer ce suivi, le CEN et le CENELEC pourraient mettre en place un processus formel d'identification et de documentation des divergences, s'appuyant sur l'expertise fine des comités techniques impliqués. En parallèle, un mécanisme de contrôle devrait surveiller l'impact des nouvelles versions de normes internationales qui ne sont pas encore adoptées en Europe, afin d'examiner si ces évolutions posent problème vis-à-vis des exigences réglementaires de l'UE ou de ses choix technologiques stratégiques. Cette approche proactive permettrait d'anticiper les ajustements nécessaires (par exemple, décider de développer une annexe européenne spécifique à une norme ISO nouvellement révisée, si cette révision s'écarte des besoins de l'UE) et de garantir que les décisions en matière de normalisation s'appuient sur une analyse technique approfondie tenant compte des réalités industrielles européennes. En somme, à l'ère d'une recomposition géopolitique rapide, où la bataille des standards fait rage notamment autour des données géographiques numériques, l'Union européenne doit affûter ses outils de pilotage normatif pour rester un agent structurant dans ces luttes de pouvoir.

Ainsi, l'Union européenne accorde une importance croissante aux normes. Toutefois, comme mentionné dans la première partie de cette thèse, la sensibilisation et la formation à la normalisation

[903] Ibid

restent limitées. L'enseignement formel et la formation professionnelle dans ce domaine sont peu répandus. De nombreuses entreprises européennes, qu'elles soient de grande ou petite taille, n'ont pas de démarche structurée ni de vision stratégique concernant la normalisation, et sous-estiment son rôle clé dans leurs activités économiques, qu'il s'agisse de conformité réglementaire, d'accès aux marchés ou de stratégie commerciale globale. Le bon fonctionnement du système de normalisation européen repose sur l'implication d'experts issus de secteurs variés, industrie, administration publique, sociétés civiles, monde académique et recherche. Ces spécialistes sont essentiels pour traiter les différentes problématiques liées à l'élaboration des normes. Afin de consolider la position de l'Europe sur la scène internationale et de soutenir le développement du marché unique des données numériques, il est impératif de renforcer la formation des experts en normalisation. Pour répondre à cet enjeu, le Forum de haut niveau sur la normalisation européenne (HLF) a proposé en 2023 plusieurs mesures visant à améliorer l'enseignement supérieur en normalisation au sein de l'Union européenne. Les organisations membres ont pris l'engagement de proposer des formations aux étudiants et jeunes diplômés, notamment à travers des stages[904]. Ces opportunités pourraient être offertes aussi bien par les membres du Forum que par les entreprises et institutions qu'ils représentent. L'un des objectifs est d'encourager la participation des étudiants aux travaux de normalisation, tout en menant des campagnes de sensibilisation auprès des établissements d'enseignement ainsi que des entreprises, y compris au niveau des dirigeants. Par ailleurs, il est suggéré d'intégrer des modules dédiés à la normalisation dans les cursus universitaires en commerce, droit ou ingénierie. Ces formations s'adresseraient aussi bien aux universités de recherche (niveau licence et master) qu'aux autres établissements d'enseignement supérieur[905]. Bien que cet engagement ait été pris par les membres du Forum, il demeure un engagement volontaire, sans contrainte juridique pour les pays signataires[906]. Si cette initiative témoigne d'une prise de conscience encourageante, elle met également en évidence le chemin restant à parcourir pour doter l'Europe d'un nombre suffisant d'experts en normalisation, indispensables dans tous les secteurs techniques stratégiques. De plus, les problèmes de l'harmonisation des normes européennes et de l'éducation universitaire en matière de normalisation ne sont qu'une partie des problèmes qui affectent aujourd'hui la compétitivité des normes européennes. Les facteurs financiers sont des causes importantes pour le manque de participation de beaucoup d'acteurs européens aux processus de normalisation. L'inclusion des TPE et PME européennes reste un défi important pour l'Europe. Pourtant, une plus grande inclusivité pourrait être un facteur décisif pour maintenir la compétitivité des acteurs européens au sein des instances internationales de normalisation.

---

904 High Level Forum on European Standardisation, « High – Level Forum recommendations on increasing funding for standardisation activities at international level », 11 novembre 2024.

905 High-Level Forum on European Standardisation, « Education & Skills on Standards », 30 novembre 2023, p. 3.

906 Ibid

1.2 L'Union européenne au défi du renouvellement de sa stratégie en matière de normalisation internationale

La question du financement des experts se pose avec d'autant plus d'acuité dans un contexte où de nombreux gouvernements européens cherchent à maîtriser leurs dépenses publiques. L'augmentation des budgets alloués à la défense à l'échelle du continent exerce une pression supplémentaire sur les financements destinés à d'autres secteurs. Lors de la seconde réunion du HLF, tenue le 30 novembre 2023, il a été reconnu que le manque de ressources constituait un frein majeur à la participation et à l'influence de l'Union européenne dans les instances internationales de normalisation[907]. Cette constatation s'inscrivait dans le cadre d'une enquête menée par le HLF visant à renforcer la présence européenne dans l'élaboration des normes internationales. Plusieurs problématiques ont été mises en avant. En premier lieu, la pénurie de ressources financières et humaines entrave la capacité des entreprises européennes à défendre efficacement leurs intérêts dans le processus de normalisation. Par ailleurs, les démarches administratives lourdes, associées à des coûts élevés et à une complexité accrue, limitent l'accès aux financements nécessaires pour permettre aux experts de mener à bien leurs travaux de normalisation dans des délais raisonnables. De plus, le besoin d'une représentation accrue de l'Union européenne au sein des comités techniques, sous-comités et groupes de travail dans les domaines stratégiques a également été mis en exergue. Cette représentation devrait inclure une diversité d'acteurs issus du secteur économique ainsi que des parties prenantes de la société civile. L'influence européenne ne devrait pas se limiter au rôle d'organisateur ou de gestionnaire de secrétariat au sein des instances nationales de normalisation, mais nécessite un engagement plus actif et structuré de la part des organismes nationaux et des experts industriels européens au sein des différents groupes de travail. Enfin, il faut garder à l'esprit que la capacité d'influence repose sur deux éléments fondamentaux. Tout d'abord, la qualité des experts techniques représentant l'UE, et une participation élargie du monde universitaire et des industriels, permettant de proposer de nouveaux sujets, de défendre des avancées techniques et de peser sur le contenu des normes en cours d'élaboration [908].

Le HLF également a mis en lumière plusieurs défis majeurs entravant l'efficacité et la coordination des efforts en matière de normalisation en Europe[909]. Tout d'abord, il existe une hétérogénéité marquée dans les critères d'évaluation des priorités de normalisation à travers les différents programmes de financement, ce qui complique la mise en cohérence des actions menées. De

---

907 High Level Forum on European Standardisation, « High – Level Forum recommendations on increasing funding for standardisation activities at international level », 11 novembre 2024.

908 European Parliamentary Research Service, « Key enabling technologies for Europe's technological sovereignty », Scientific Foresight Unit (STOA), PE 697.184, décembre 2021, pp. 113, p. 16.

909 High Level Forum on European Standardisation, « High – Level Forum recommendations on increasing funding for standardisation activities at international level », 11 novembre 2024.

plus, le lien entre les travaux de prénormalisation et la participation effective aux comités techniques demeure flou, ce qui limite l'impact des initiatives en amont sur l'élaboration des normes. Un autre obstacle réside dans l'absence de coordination entre les activités de normalisation et les besoins concrets des secteurs industriels et des applications technologiques. Cette déconnexion freine l'intégration des innovations issues du monde industriel dans le processus de normalisation. Par ailleurs, de nombreuses organisations, notamment les PME, les universités et les instituts de recherche, peinent à financer la participation de leurs experts aux travaux des comités de normalisation. Cette difficulté est d'autant plus problématique qu'elle affecte directement la capacité de l'Union européenne à soutenir ses cadres législatifs et à développer des standards alignés avec ses priorités stratégiques en matière de politique industrielle. Les écarts entre les États membres en termes de capacité de financement et de participation active aux travaux de normalisation constituent également un frein important. Ces disparités contribuent à un déséquilibre dans l'élaboration des normes, certains pays étant mieux représentés et plus influents que d'autres. Dans le même temps, les entreprises européennes font face à un besoin croissant de main-d'œuvre qualifiée, notamment dans les technologies critiques. L'intégration des compétences en normalisation dans les formations techniques et professionnelles apparaît aujourd'hui comme capital pour garantir un développement industriel compétitif. En outre, les lourdeurs administratives associées aux processus de normalisation dissuadent de nombreux acteurs de s'impliquer pleinement, générant ainsi des retards inutiles et freinant l'évolution des normes. Enfin, de nombreux programmes de financement et partenariats de l'UE dédiés à l'innovation industrielle, au développement et au déploiement restent sous-exploités. Ces dispositifs ne considèrent pas toujours la normalisation et la participation aux comités techniques comme des activités éligibles au financement, ce qui constitue un frein supplémentaire au développement des travaux de normalisation internationaux en matière de normes géographiques. Cette situation limite la valorisation des résultats des projets de recherche et de développement, alors qu'une meilleure intégration de la normalisation dans ces programmes permettrait d'assurer une adoption plus rapide des avancées technologiques et d'accroître l'influence européenne sur la scène internationale.

De plus en plus d'initiatives nationales à travers l'Europe témoignent d'une prise en compte des facteurs financiers limitant l'implication dans la normalisation internationale. La France apparaît aujourd'hui comme un des meilleurs élèves de l'Union. Ainsi le rapport du HLF cite plusieurs mesures françaises comme étant des bonnes pratiques, comme le décret français sur la normalisation[910] qui a mis en place une participation gratuite aux comités de normalisation pour les petites et moyennes entreprises, les parties prenantes de la société (consommateurs, associations environnementales, syndicats) et le monde universitaire. De plus, le gouvernement français et l'AFNOR ont signé en 2023

[910] Décret n° 2009-697 du 16 juin 2009 relatif à la normalisation.

un partenariat[911] visant à encourager la participation aux activités de normalisation pour les bénéficiaires du plan d'investissement France 2030. Le Crédit d'Impôt Recherche[912] offre également des réductions d'impôts aux entreprises engagées dans des activités de recherche, d'innovation et de développement, y compris la normalisation. Il existe également plusieurs plans d'action paneuropéens pour renforcer la présence des experts européens en normalisation dans divers domaines techniques. Parmi eux, le projet Cyberstand[913] vise à permettre aux parties prenantes européennes de s'engager dans le développement de normes et de conformité en relation avec la loi sur la cyberrésilience (Cyber Resilience Act)[914]. Selon le LHF, ce projet sélectionnera et engagera plus de 200 experts à travers 6 cycles de procédures de services spécifiques (SSP), attribuant un total de 1.500.000 € pour le développement et le travail sur des normes harmonisées[915]. L'argent reste le nerf de la guerre, et force est de constater que les contraintes économiques pèsent encore lourdement sur l'implication des différents acteurs européens dans la standardisation internationale.

Ces contraintes financières révèlent une géographie inégalitaire de l'accès aux arènes normatives internationales, où la capacité à peser sur l'élaboration des standards devient un privilège réservé aux acteurs disposant de ressources suffisantes pour maintenir une présence continue dans les instances de normalisation. Les PME et TPE européennes se trouvent ainsi marginalisées dans des espaces de pouvoir technique dont elles subissent pourtant les effets sur leurs territoires d'activité, créant une asymétrie structurelle entre ceux qui font les normes et ceux qui les appliquent. Cette exclusion géographique et économique des petits acteurs fragilise la représentativité du système normatif européen et, par ricochet, affaiblit la capacité de l'Union à projeter ses intérêts dans les négociations internationales face à des puissances où la concentration industrielle permet une mobilisation normative plus efficace.

La rhétorique européenne sur le rôle stratégique des normes internationales dans la réduction des barrières commerciales masque en réalité un enjeu géopolitique majeur : le contrôle des référentiels techniques qui structurent l'accès aux marchés mondiaux constitue un instrument de domination économique à l'échelle globale. En intégrant pleinement les normes internationales dans son cadre réglementaire, l'Union européenne ne se contente pas d'harmoniser des pratiques, elle participe à une

---

911 https://www.info.gouv.fr/actualite/france-2030-signature-d-un-partenariat-afnor-sgpi-et-dge-pour-developper-un-usage-strategique-de-la

912 https://entreprendre.service-public.fr/vosdroits/F23533

913 https://cyberstand.eu/

914 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847.

915 High Level Forum on European Standardisation, « High – Level Forum recommendations on increasing funding for standardisation activities at international level », 11 novembre 2024.

compétition géopolitique pour définir les règles du jeu de la mondialisation. La « Stratégie de normalisation » de 2022[916] ne laisse aucun doute sur cette dimension stratégique. La souveraineté technologique européenne et la réduction de ses dépendances économiques passent par la capacité de ses acteurs à imposer leurs standards dans les arènes internationales, transformant ainsi la normalisation en un front géoéconomique où se joue l'autonomie du continent.

Cependant, cette ambition se heurte à une contradiction fondamentale : comment l'Europe peut-elle prétendre à une puissance normative mondiale tout en excluant structurellement une partie significative de son tissu économique des processus de standardisation ? L'« approche inclusive » revendiquée par Bruxelles, censée mobiliser industries, administrations, société civile et monde académique[917], demeure ainsi largement théorique tant que persistent les barrières financières et organisationnelles qui confinent la normalisation aux grandes entreprises et aux capitales nationales. Cette géographie concentrée du pouvoir normatif européen contraste avec les stratégies d'autres puissances, notamment la Chine, qui ont su mobiliser massivement leurs acteurs économiques, y compris les PME, dans une politique industrielle intégrée où la normalisation devient un levier coordonné de projection géopolitique.

La participation des PME et de la société civile aux processus de normalisation ne constitue donc pas simplement un enjeu de représentativité démocratique, mais un impératif géostratégique pour l'Europe. Dans un contexte de fragmentation croissante des espaces normatifs mondiaux, où chaque bloc géopolitique tente d'imposer ses propres référentiels, la capacité de l'Union à mobiliser l'ensemble de son écosystème économique et social détermine son poids dans les rapports de force normatifs internationaux. L'enjeu n'est plus seulement de former une « nouvelle génération d'experts », mais de construire une véritable infrastructure géopolitique de la normalisation, capable de projeter les valeurs et les intérêts européens dans les standards qui régissent les flux de marchandises, de technologies et de données à l'échelle planétaire. Sans cette mobilisation territoriale élargie, l'Europe risque de se trouver dans une position défensive, contrainte d'adopter des normes élaborées ailleurs, dans des arènes où elle n'aura pas su ou pu être présente avec suffisamment de force.

Comme le rappel le rapport du chantier n°5 du HLF, consacré à l'inclusion de la société civile et des PME dans la normalisation internationale[918], l'entrée en vigueur du règlement 1025/2012[919], a fait de l'inclusivité un pilier central du Système européen de Normalisation, mettant en avant l'importance

---

916 Communication From The Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, « An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market », Brussels, 2.2.2022, COM(2022) 31 final, p. 3. https://ec.europa.eu/docsroom/documents/48598. Consulté le 7 janvier 2023, p. 3.

917 European Commission, « Joint Initiative on Standardisation under the Single Market Strategy », 20 août 2018, p. 12.

918 High – Level Forum on European Standardisation, « Greater civil society and SME inclusion in international standardisation. Mapping, analysis and recommandations for greater civil society inclusion in standardisation at international level » , rapport du chantier n°5 (pilote : ECOS), janvier 2025.

des parties prenantes issues de la société civile ainsi que des PME. Afin de renforcer cette approche, plusieurs mesures ont été mises en place, notamment à travers le guide 25 du CEN-CENELEC[920], qui définit précisément les rôles et responsabilités des organisations partenaires. Ce cadre leur permet d'intégrer pleinement les comités techniques et les groupes de travail, leur offrant ainsi une voix active dans l'élaboration des normes. Pour aller plus loin, des initiatives spécifiques ont été mises en place afin de mieux répondre aux attentes des parties prenantes. Le groupe de travail sur les PME (SME WG) et le groupe des parties prenantes sociétales (SSG) ont été créés dans cette optique, offrant des espaces de dialogue et de collaboration plus directs. L'une des avancées majeures du SSG a été l'introduction d'un droit d'opinion[921] permettant aux organisations de la société civile, telles que ECOS[922], ANEC[923] et ETUC[924], ainsi qu'aux PME, représentées par SBS[925], d'émettre un avis formel sur un projet de norme lors des phases d'enquête et de vote formel. Afin de garantir un accès équitable à l'information et de favoriser la participation des acteurs concernés, des supports de formation et diverses publications ont été développés à destination des organisations de la société civile et des PME. De plus, l'ouverture de l'accès en ligne aux documents normatifs pour ces organisations constitue une avancée significative vers un système plus transparent et inclusif. Toutefois, cette mesure ne s'applique pas encore aux normes internationales, même lorsqu'elles sont adoptées au niveau européen. Cet engagement progressif de l'Europe démontre néanmoins une volonté claire de continuer à élargir l'accès à la normalisation et de garantir la représentativité de toutes les parties prenantes dans ce processus essentiel.

L'ISO, en collaboration avec la CEI, le CEN et le CENELEC, a adopté la Déclaration de Londres le 24 septembre 2021[926] afin de s'assurer que les normes internationales jouent un rôle clé dans la lutte contre le changement climatique. Cette initiative vise également à renforcer l'implication de la société civile et des populations les plus vulnérables aux effets du climat dans l'élaboration des normes et des publications internationales. Dans cette perspective, la Déclaration de Londres représente une

---

919 Règlement (UE) n ° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n ° 1673/2006/CE du Parlement européen et du Conseil Texte présentant de l'intérêt pour l'EEE https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32012R1025

920 CEN-CENELEC, « GUIDE 25 : The concept of Cooperation with European Organizations and other stakeholders », (3), novembre 2021.

921 European Commission, « SMEs and standardisation in Europe », EIM Business & Policy Research, Zoetermeer, Octobre 2006.

922 Environmental Coalition on Standards.

923 The European Association for the Coordination of Consumer Representation in Standardisation.

924 European Trade Union Confederation

925 Small Business Standard.

926 ISO, « Déclaration de Londres: l'ISO s'engage à agir en faveur du climat », 24 septembre 2021. https://www.iso.org/fr/news/ref2726.html. Consulté le 12 janvier 2025.

opportunité précieuse pour améliorer l'inclusivité au sein des processus de normalisation de l'ISO et de la CEI. Une telle évolution pourrait être portée par les organismes nationaux de normalisation (ONN) européens, qui jouent un rôle essentiel dans le système régional, afin de garantir une représentation plus équitable des différents acteurs. Cette question revêt une importance particulière lorsque des normes définies à l'échelle internationale sont ensuite adoptées comme normes européennes, dans le but de soutenir la législation de l'Union européenne. Dans ce contexte, il est impératif que les exigences fixées par le règlement (UE) n° 1025/2012, notamment en matière d'inclusivité, soient entièrement respectées. Toutefois, des disparités subsistent entre les niveaux européen et international en ce qui concerne l'implication des PME et des organisations représentant les parties prenantes de la société. Alors qu'en Europe, ces acteurs bénéficient d'un soutien financier et de droits d'accès aux comités techniques et aux groupes politiques concernés, le système international fonctionne différemment. L'accès aux processus de normalisation y est soumis à des demandes spécifiques et à des procédures d'approbation au cas par cas, que ce soit au niveau technique ou dans le cadre de l'élaboration des politiques. Dans ce contexte, les normes harmonisées issues des instances internationales pourraient ne pas toujours refléter les principes d'inclusivité appliqués en Europe. Il est donc essentiel d'assurer un alignement entre les pratiques de normalisation internationales et les exigences européennes afin de garantir que les normes adoptées respectent les valeurs et les principes qui régissent le Système européen de Normalisation (SEN).

Le même rapport souligne que l'une des principales forces du système européen de normalisation en matière de participation aux instances internationales réside dans son modèle de délégation nationale[927], un principe partagé qui structure son fonctionnement et qui, contrairement aux approches plus centralisées observées ailleurs, préserve la diversité des expertises nationales tout en permettant une coordination stratégique[928]. Ce modèle confère à l'Europe un avantage distinctif : la capacité à mobiliser une pluralité d'acteurs économiques et sociaux dont l'expérience collective enrichit les positions défendues dans les arènes internationales. Ainsi, toute initiative visant à renforcer la participation des organismes nationaux de normalisation (ONN) et des Comités nationaux (CN) au sein de ce système aura également pour effet de consolider leur influence dans les processus de normalisation menés au niveau de l'ISO et de la CEI.

Dans cette perspective, l'existence d'un cadre réglementaire européen dédié à la normalisation, notamment à travers le règlement 1025/2012 qui impose des exigences d'inclusivité absentes des

---

927 High – Level Forum on European Standardisation, « Greater civil society and SME inclusion in international standardisation. Mapping, analysis and recommandations for greater civil society inclusion in standardisation at international level » , rapport du chantier n°5 (pilote : ECOS), janvier 2025.

928 Contrairement au modèle centralisé chinois où la Standardization Administration of China (SAC) coordonne l'ensemble des positions nationales, le système européen repose sur une coordination entre organismes nationaux autonomes, préservant ainsi une pluralité d'expertises sectorielles et territoriales.

systèmes internationaux[929], constitue un levier essentiel pour encourager l'implication structurée des acteurs européens sur la scène internationale. Ce cadre favorise la mise en place de mesures stratégiques visant à accroître la présence et l'impact des organisations européennes dans l'élaboration des normes mondiales, tout en garantissant une représentation équilibrée des parties prenantes. L'approche inclusive promue par l'Union européenne, qui intègre explicitement les PME, les organisations de la société civile et le monde académique dans les processus de normalisation, représente une spécificité européenne que d'autres systèmes nationaux ne peuvent égaler[930]. Cette diversité d'acteurs, loin de constituer une faiblesse, offre à l'Europe une légitimité démocratique dans ses positions normatives, renforçant la crédibilité de ses propositions face à des approches plus dirigistes où la normalisation demeure l'apanage d'acteurs étatiques ou de grandes entreprises. Par ailleurs, le développement de structures spécialisées, de réseaux professionnels, groupes politiques et comités sectoriels, représente un atout supplémentaire pour soutenir l'influence européenne au sein de l'ISO et de la CEI. L'écosystème normatif européen bénéficie également d'une tradition d'excellence technique héritée de décennies de collaboration entre organismes nationaux de normalisation, qui ont su développer des méthodologies de travail robustes et des standards de qualité reconnus internationalement. Cette expertise technique constitue un capital normatif considérable que l'Europe peut mobiliser dans les négociations internationales.

Le principal enjeu d'amélioration du système européen réside dans l'élargissement effectif de sa base participative. Bien que les ONN et les CN aient développé des initiatives efficaces au niveau national, telles que les dispositifs français de participation gratuite pour les PME et le Crédit d'Impôt Recherche, ou le projet paneuropéen Cyberstand[931], la participation des PME et des organisations de la société civile aux processus de normalisation européens et internationaux demeure entravée par des barrières financières structurelles. Les coûts de déplacement, le temps de participation et l'expertise spécialisée requise[932] créent une géographie inégalitaire où seules les grandes entreprises et certaines capitales disposent des ressources nécessaires pour peser durablement sur l'élaboration des standards internationaux.

---

929 Le règlement (UE) 1025/2012 impose des exigences explicites d'inclusivité (articles 5 et 6) qui ne trouvent pas d'équivalent dans les règlements ISO ou IEC, conférant au système européen une dimension démocratique distinctive.

930 High-Level Forum on European Standardisation (2024). "WORKSTREAM 3 NSBs peer-review", septembre 2024. 57% des ONN européens incluent des représentants des PME et de la société civile de manière permanente dans leurs structures dirigeantes.

931 Voir la section 1.2 du présent chapitre sur les initiatives nationales françaises (participation gratuite, Crédit d'Impôt Recherche, partenariat France 2030-AFNOR) et le projet paneuropéen Cyberstand (200 experts, budget de 1,5M€)

932 De Vries, H. et al. (2009). "SME access to European standardization: Enabling small and medium-sized enterprises to achieve greater benefit from standards and from involvement in standardization", ResearchGate, août 2009.

Cette situation représente un handicap géostratégique pour l'Europe. En effet, les PME européennes, qui constituent 99% des entreprises et fournissent deux tiers des emplois du secteur privé[933], demeurent largement absentes des arènes normatives internationales en raison de contraintes de ressources[934], alors même que leur participation serait cruciale pour ancrer les normes dans les réalités diversifiées du tissu économique européen et pour contrebalancer l'influence croissante d'acteurs qui mobilisent l'ensemble de leur écosystème industriel. L'approche inclusive revendiquée par Bruxelles, si elle reste au stade du principe sans mécanismes effectifs de compensation des inégalités d'accès[935], ne pourra pleinement déployer le potentiel normatif européen face à des puissances qui ont compris que le contrôle des infrastructures normatives constitue un instrument de domination géoéconomique.

Il reste donc essentiel de poursuivre les efforts pour garantir une représentation plus équilibrée et assurer que l'ensemble des parties prenantes puissent pleinement contribuer aux décisions normatives qui façonnent les marchés internationaux. L'enjeu n'est pas simplement d'améliorer l'inclusivité du système pour des raisons de légitimité démocratique, bien que cet objectif demeure fondamental, mais de transformer cette inclusivité en avantage stratégique géopolitique. En mobilisant effectivement l'ensemble de son écosystème économique et social, des PME aux grandes entreprises, des territoires périphériques aux centres de décision, de la société civile au monde académique, l'Europe peut transformer sa diversité structurelle en force de projection normative, capable de défendre ses intérêts économiques, ses valeurs réglementaires et son autonomie stratégique face aux dynamiques de recomposition de l'ordre normatif mondial. Cette capacité à conjuguer excellence technique, légitimité démocratique et coordination stratégique constitue la voie par laquelle l'Europe peut non seulement préserver son influence dans les instances internationales, mais également proposer un modèle alternatif de gouvernance normative qui réconcilie efficacité géopolitique et principes d'ouverture.

Le rapport du chantier n°5 indique bien que les organismes nationaux de normalisation européens comprennent l'importance d'impliquer toutes les parties prenantes dans la normalisation, y compris la société civile et les PME, et la nécessité de continuer à progresser. Bien qu'il n'ait pas été possible de compiler des données sur la répartition proportionnelle des parties prenantes dans les TC au niveau national, les données du chantier n° 3 du HLF montrent que *« en ce qui concerne la participation des représentants des parties prenantes aux structures dirigeantes et/ou aux organes*

933 Toffaletti, S. (2016). "European SMEs and Standards", ASTM Standardization News.

934 ISO (2013). "Improving SME access to standards", février 2013. L'étude néerlandaise révèle que la raison principale de non-participation des PME à la normalisation est souvent simplement qu'elles ne connaissent pas l'existence de ce processus.

935 Small Business Standards (2022). "SBS welcomes early phase of the standardization strategy implementation", CEN-CENELEC, 16 novembre 2022. SBS souligne qu'un obstacle majeur à la participation des PME reste la disponibilité des ressources, appelant à un soutien financier accru aux niveaux national et européen.

consultatifs, 57 % des ONN incluent des représentants des PME et des parties prenantes de la société de manière permanente dans ces structures, tandis que 27 % n'ont pas pris de telles mesures. Environ 25 % créent des organes consultatifs visant à discuter des questions concernant les parties prenantes sous-représentées (similaires aux groupes CEN-CENELEC pour les PME ou les parties prenantes sociétales) ou invitent ces parties prenantes aux réunions des organes directeurs ou consultatifs sur une base ad hoc »[936]. Les résultats indiquent qu'il y a une marge d'amélioration également de la part des autres parties prenantes de la normalisation européenne, telles que les partenaires sociétaux et les PME, ainsi que les États membres. En outre, l'identification et l'engagement des parties prenantes de la société et des PME au niveau national doivent également être renforcés. Tous ces éléments montrent qu'il existe une lacune dans l'inclusion des organisations nationales représentant les intérêts des parties prenantes de la société et dans le bon fonctionnement du SEN fondé sur le principe de la délégation nationale, à partir de laquelle les ONN et les CN organisent et canalisent la participation aux travaux de normalisation européens et internationaux.

Ainsi, comme le souligne le rapport, contrairement à ce qui se passe dans le contexte européen, où des représentants de la société civile ont accès aux comités techniques ainsi qu'aux groupes de travail du CEN-CENELEC, selon le règlement 1025/2012, leur représentation au sein des comités techniques internationaux n'est pas garantie[937]. Leur admission repose sur un processus d'approbation spécifique, où chaque demande de liaison est examinée individuellement et soumise au vote des membres nationaux du comité concerné. Cette procédure implique des critères d'éligibilité stricts, qui peuvent représenter un obstacle supplémentaire pour les organisations souhaitant obtenir ce statut. Plus encore, un rejet de candidature signifie une exclusion complète du processus de normalisation international, empêchant ainsi l'organisation concernée de contribuer aux travaux du comité. Cette situation a notamment touché des structures comme ECOS, ETUC et SBS, dont les demandes de liaison ont été refusées par certains comités techniques de l'ISO et de la CEI, restreignant leur capacité à influencer l'élaboration des normes à l'échelle mondiale[938]. Afin de surmonter ces difficultés, il serait pertinent d'adopter une approche plus proactive de la part des organismes nationaux de normalisation et des comités nationaux européens. Un vote favorable, plutôt qu'une abstention, lors des décisions relatives aux demandes de liaison pourrait significativement améliorer les chances d'acceptation de ces organisations. Un tel soutien permettrait de garantir une représentation plus équilibrée des acteurs européens et de renforcer leur influence dans les processus de normalisation internationale.

---

936 High-Level Forum on European Standardisation, « WORKSTREAM 3 NSBs peer-review (including SMEs and civil society inclusiveness) – REPORT Summary of findings from the questionnaires and interviews », septembre 2024. p. 13. https://ec.europa.eu/docsroom/documents/61814. Consulté le 18 novembre 2024.

937 Ibid

938 ECOS, « The IEC shuts the door to environmental organisations (again!) », 30 mai 2019. https://ecostandard.org/news_events/the-iec-shuts-the-door-to-environmental-again/. Consulté le 20 mars 2024.

Le même rapport relève également que le processus d'adoption d'une demande de liaison dans le cadre de la normalisation internationale se révèle souvent long et complexe. En effet, actuellement les directives ISO/IEC ne fixent aucun délai pour le traitement ds demandes de liaison, ce qui entraîne des retards susceptibles de faire manquer des étapes clés de l'élaboration de normes. Il souligne aussi le coût de la participation aux travaux internationaux. En effet, si les entreprises y voient un investissement, qui leur permet de contribuer aux références techniques dont dépend leur compétitivité, les organisations de la société civile, qui ne vendent ni produits, ni services, ne peuvent participer qu'à la condition de bénéficier de financements dédiés, souvent insuffisants lorsque les réunions se tiennent sur tous les continents[939].

Enfin, le rapport note que les conditions dans lesquelles des normes harmonisées, élaborées en réponse à des demandes de normalisation de la Commission ,sont développées sous la direction de l'ISO ou de la CEI, relèvent des accords de Vienne et de Francfort et du règlement intérieur du CEN – CENELEC (partie 2), mais que les moyens d'y garantir une participation équilibrée restent « non documentés et flous ». La révision des lignes directrices d'applicaiton de l'accord de Vienne et la mise à jour annuelle du règlement intérieur pourraient en fournir l'occasion, alors que le Vade – mecum sur la normalisation européenne n'en fait pas mention[940].

De plus, le rapport rappelle que le règlement 1025/2012, qui encadre les travaux réalisés en lien avec les demandes de normalisation, s'applique indépendamment de leur origine. Toutefois, son application effective au niveau international soulève certaines interrogations. Certaines dispositions, notamment celles relatives à l'inclusivité, pourraient être difficiles à mettre en œuvre lorsque la normalisation est externalisée à l'ISO ou à la CEI. En conséquence, l'alignement entre les pratiques européennes et internationales en matière de normalisation apparaît incohérent, notamment concernant l'implication des organisations sociétales et des PME. Si l'article 6 du règlement assure une couverture aux PME, les autres parties prenantes sociétales ne bénéficient pas du même cadre structuré, et leur participation dépend largement du soutien financier apporté par les États membres à leurs organisations nationales. De plus, comme l'ont souligné Eliantonio et Volpato (2022)[941], ni le règlement 1025/2012 ni les contrats entre la Commission européenne (CE) et un Organisme européen de Normalisation (OEN) ne précisent clairement les conditions dans lesquelles une décision d'externalisation du processus de normalisation peut être prise à l'échelle internationale. Le Vade-mecum n'apporte pas non plus

---

939 High-Level Forum on European Standardisation, « WORKSTREAM 3 NSBs peer-review (including SMEs and civil society inclusiveness) – REPORT Summary of findings from the questionnaires and interviews », septembre 2024. p. 11. https://ec.europa.eu/docsroom/documents/61814. Consulté le 18 novembre 2024

940 Ibid, p. 12

941 Eliantonio, M. et Volpato Annalisa, « The European System of Harmonised Standards. Legal Opinion for ECOS », 11 mars 2022. Disponible ici: https://ssrn.com/abstract=4055292 ou http://dx.doi.org/10.2139/ssrn.4055292. Consulté le 20 mars 2024.

d'éclaircissements sur les mécanismes régissant ce transfert des travaux de normalisation vers des instances internationales, laissant un flou sur qui prend ces décisions, à quel moment et selon quelles modalités.

Cette situation pose un défi supplémentaire, puisque les différences d'accès aux instances de normalisation entre le niveau européen et international risquent de compromettre le principe de primauté des normes internationales pour les PME européennes et les organisations de la société civile. Il devient donc impératif d'améliorer l'inclusivité au sein des instances internationales, afin de garantir que toutes les parties prenantes aient la possibilité de contribuer efficacement à l'élaboration des normes. Cet enjeu est d'autant plus critique que le Système européen de Normalisation (SSE) repose sur un principe d'ouverture, visant à intégrer toutes les voix concernées dans le processus normatif. Une approche plus structurée et plus transparente est donc nécessaire pour assurer un équilibre entre les intérêts industriels et sociétaux, tant au niveau européen qu'international.

1.3 Les espaces communs de données : normaliser pour transcender les frontières européennes et exploiter au mieux les données des pays membres

Pour comprendre ce que sont les espaces communs de données européens, imaginons un instant le fonctionnement d'un marché traditionnel. Sur ce marché, différents producteurs apportent leurs produits : certains vendent des fruits, d'autres du fromage, d'autres encore des légumes. Pour que ce marché fonctionne efficacement, il faut un lieu commun (la place du marché), des règles partagées (horaires d'ouverture, normes sanitaires, système de paiement), et une organisation permettant à chacun de présenter ses produits de manière compréhensible pour les acheteurs. Les espaces communs de données européens (ou Common European Data Spaces) fonctionnent selon une logique similaire. Ils créent des « places de marché numériques » sectorielles où différentes organisations peuvent mettre à disposition, échanger et utiliser des données de manière sécurisée, tout en conservant le contrôle sur leurs propres informations[942].

Plus précisément, un espace commun de données se définit comme un écosystème numérique fédéré qui rassemble trois composantes essentielles[943]. Premièrement, une infrastructure technique commune permettant le stockage, l'accès et l'échange sécurisé de données entre participants (connecteurs, systèmes d'authentification, catalogues, services de gestion des licences). Deuxièmement,

[942] Commission européenne (2022). "Staff Working Document on common European data spaces", SWD(2022) 45 final, janvier 2024.

[943] Data Spaces Support Centre (DSSC), Glossaire officiel. Un espace de données est défini comme *"un système distribué encadré par une gouvernance permettant des transactions sécurisées entre les participants, tout en garantissant la confiance et la souveraineté des données."*

un cadre de gouvernance partagé établissant les règles d'accès, d'utilisation et de partage des données, ainsi que les mécanismes garantissant la confiance entre participants. Troisièmement, une communauté d'acteurs appartenant à un même secteur ou domaine d'intérêt qui acceptent de coopérer autour d'objectifs communs liés à la valorisation des données. Contrairement à une simple plateforme centralisée (comme un "data lake" unique), un espace de données repose sur une architecture distribuée où chaque participant conserve le contrôle de ses propres données tout en pouvant les rendre accessibles selon des conditions qu'il définit lui-même[944].

L'Union européenne a lancé le développement de quatorze espaces communs de données dans des secteurs stratégiques de l'économie et de la société[945]. Parmi eux, l'espace européen des données de santé (European Health Data Space, EHDS), qui est le premier à avoir émergé sous forme de proposition réglementaire en 2024[946], vise à permettre aux citoyens européens d'accéder à leurs dossiers médicaux électroniques partout dans l'UE et de faciliter le partage sécurisé de données de santé pour la recherche médicale, tout en garantissant le respect de la vie privée. L'espace de données agricoles permettra aux agriculteurs de comparer les performances de leurs exploitations avec d'autres fermes européennes pour améliorer leur durabilité et leur compétitivité économique[947]. L'espace de données de mobilité facilitera la gestion de la logistique intermodale dans le transport de marchandises et optimisera les déplacements personnels en combinant données routières, ferroviaires et aériennes[948]. D'autres espaces couvrent des domaines aussi variés que l'énergie, l'industrie manufacturière, la finance, le Green Deal, l'administration publique, le patrimoine culturel, les compétences professionnelles (skills), le tourisme, les médias ou encore la recherche et l'innovation[949].

Dans le domaine géospatial qui nous intéresse particulièrement, l'initiative Destination Earth (DestinE), rattachée à l'espace commun de données du Green Deal, illustre concrètement cette approche. Ce projet développe un modèle numérique haute précision de la Terre permettant à des utilisateurs, y compris des non-spécialistes scientifiques, d'accéder et d'interagir avec d'immenses

---

944 Commission européenne (2024). "When open data meets data spaces", data.europa.eu. Les espaces de données ne sont ni de simples "data lakes", ni de simples catalogues, ni uniquement des infrastructures techniques – ils combinent technologie, gouvernance et communauté.

945 Commission européenne (2024). "Common European data spaces", Shaping Europe's digital future. 14 espaces sont en développement : agriculture, patrimoine culturel, énergie, finance, Green Deal, santé, industrie, langues, médias, mobilité, administration publique, recherche et innovation, compétences, tourisme.

946 Arthur Cox LLP (2024). "What are Common European Data Spaces?", juillet 2024. L'European Health Data Space (EHDS) a été provisoirement approuvé en mars 2024 par le Conseil de l'UE et le Parlement européen, devenant le premier espace sectoriel spécifique à émerger.

947 Commission européenne (2024). "Common European data spaces", op. cit. L'espace agricole vise à *"améliorer la performance en matière de durabilité et la compétitivité du secteur agricole grâce au traitement et à l'analyse des données."*

948 Ibid. L'espace mobilité vise à *"positionner l'Europe à l'avant-garde du développement d'un système de transport intelligent."*

949 Liste complète disponible dans Commission européenne (2024). "Second Staff Working Document on Data Spaces", SWD(2024), janvier 2024.

volumes de données géospatiales, climatiques et socio-économiques. Les applications permettent, par exemple, de modéliser les inondations urbaines, l'exposition à la chaleur dans les villes, ou encore de calculer les risques sanitaires liés au changement climatique, autorisant ainsi des mesures politiques préventives adaptées. Cet exemple montre comment les espaces de données transcendent les frontières nationales et sectorielles. Ainsi, les données géospatiales produites par les agences nationales de cartographie, les observations satellitaires européennes (Copernicus), les données météorologiques et les statistiques socio-économiques peuvent être combinées pour produire des analyses que chaque État membre ne pourrait réaliser isolément.

La place centrale des données dans l'économie numérique européenne se traduit aujourd'hui par les initiatives menées par la Commission européenne pour encadrer leur gestion et leur partage. Ces réglementations visent à créer un écosystème de données dynamique au sein de l'Union européenne, tout en garantissant la protection des droits fondamentaux des citoyens et en préservant la souveraineté technologique du continent. Pour atteindre ces objectifs, le partage des données doit être transparent, efficace et sécurisé. Cela repose sur le respect des principes FAIR (Facilité de découverte, Accessibilité, Interopérabilité et Réutilisation), qui constituent un socle fondamental pour la mise en place d'espaces de données paneuropéens. Ce modèle s'inspire de la directive INSPIRE, qui a déjà permis d'harmoniser l'accès aux informations géospatial à l'échelle de l'UE. Les espaces de données représentent une approche clé pour favoriser et structurer le partage d'informations entre acteurs d'un même secteur. Ils se définissent comme des communautés d'organisations partageant des objectifs communs en matière de gestion et d'échange de données. Toutefois, leur développement s'effectuant de manière relativement autonome, il est essentiel d'accorder une attention particulière aux enjeux d'interopérabilité. L'harmonisation des systèmes au sein d'un espace de données, mais aussi entre différents espaces, constitue un facteur déterminant de leur succès. Ainsi, une interopérabilité accrue permet de réduire les obstacles techniques, d'encourager l'adoption d'outils mutualisés et de favoriser une intégration fluide des données par des acteurs de toutes tailles et de tous secteurs. Cette approche facilite ainsi une adoption à grande échelle et maximise l'impact des politiques européennes en matière de gouvernance des données.

Les espaces de données constituent un levier essentiel pour structurer et fluidifier le partage d'informations entre différents acteurs. Ils fonctionnent comme des écosystèmes où des communautés d'organisations se regroupent autour de jeux de données et de besoins communs liés à un secteur spécifique. Selon le glossaire du DSSC, un espace de données se définit comme un *« système distribué encadré par une gouvernance permettant des transactions sécurisées entre les participants, tout en*

garantissant la confiance et la souveraineté des données »[950]. Sur le plan technique, ces espaces intègrent divers éléments clés, tels que des connecteurs, des mécanismes d'authentification, des systèmes de catalogage ou encore des services dédiés à la gestion des licences et des contrats. Leur force réside dans leur flexibilité, qui leur permet de traiter des enjeux aussi variés que la gouvernance des données, leur valorisation, la mise en place d'un climat de confiance et le développement de communautés adaptées aux spécificités de chaque domaine. Cependant, comme ces espaces évoluent souvent de manière autonome selon les secteurs d'activité, la question de l'interopérabilité devient un enjeu central. Assurer une compatibilité entre les différentes infrastructures est un facteur déterminant de succès, car cela permet de limiter les obstacles techniques, de promouvoir l'usage d'outils mutualisés et de favoriser une adoption généralisée, quel que soit le profil des acteurs impliqués. De plus, au-delà de l'interopérabilité interne propre à chaque espace de données, il est également crucial de garantir une interconnexion efficace entre différents espaces. En effet, de nombreuses organisations sont amenées à interagir simultanément au sein de plusieurs environnements de données, nécessitant ainsi des standards communs. L'harmonisation des cadres réglementaires et techniques, incluant notamment les exigences en matière de confidentialité, de protection des données et de gouvernance, est donc essentielle. En garantissant une approche cohérente à l'échelle intersectorielle, il devient possible d'optimiser l'exploitation des volumes massifs de données générés quotidiennement et d'en maximiser la valeur.

Pour concrétiser l'ambition d'un marché unique européen des données, l'Union européenne a mis en place des espaces communs destinés à faciliter le partage et l'exploitation sécurisée d'informations stratégiques dans divers secteurs. À ce jour, quatorze espaces européens de données, soutenus par des financements de l'UE, ont été établis[951]. Ces espaces, chacun spécifique à un domaine ou à un secteur, seront progressivement interconnectés afin de constituer une infrastructure essentielle du marché unique des données. Dans cette dynamique, la Commission européenne a récemment publié un deuxième document de travail qui dresse un état des lieux de ces espaces de données en Europe[952]. L'un des leviers majeurs pour assurer leur interopérabilité réside dans l'utilisation de jeux de données de référence communs à l'ensemble des espaces. À cet égard, l'acte d'exécution relatif aux ensembles de données de grande valeur représente une avancée significative, en rendant ces données plus

---

950 Le data Space Support Center est le site officiel mis en place par l'Union Européenne pour promouvoir les espaces partagés de données au sein des États membres. La définition est disponible ici (en anglais). https://dssc.eu/space/Glossary/176554052/2.+Core+Concepts. Consulté le 5 mars 2025.

951 https://digital-strategy.ec.europa.eu/fr/policies/data-spaces

952 European Commission, « Commission Staff Working Document on Common European Data Spaces », Brussels, SWD (2024), 21 finals, 24 janvier 2024, p. 3. https://digital-strategy.ec.europa.eu/fr/library/second-staff-working-document-data-spaces. Consulté le 10 mars 2024.

largement accessibles et exploitables[953]. Les six catégories de données identifiées dans cet acte couvrent des dimensions essentielles pour de nombreux usages liés à l'analyse et au traitement des données [954]. Par exemple, les données géospatiales jouent un rôle transversal en permettant de localiser précisément les informations et d'introduire une dimension spatiale applicable à une grande diversité de domaines. Par ailleurs, les ensembles de données classés sous la catégorie « statistiques » englobent une variété d'indicateurs économiques et sociaux, offrant ainsi un socle commun pour contextualiser les analyses menées à travers les différents espaces de données. La catégorie « entreprises et propriété des entreprises » est susceptible d'être pertinente pour de nombreux espaces de données également. Le Centre de soutien aux espaces de données (DSSC)[955] est une initiative financée par le programme digital Europe[956], conçue pour apporter une assistance essentielle aux espaces de données européens communs. Son rôle principal est de coordonner les différentes actions liées aux espaces sectoriels afin d'assurer leur développement harmonisé, leur interopérabilité et leur optimisation à grande échelle. Pour atteindre ces objectifs, le DSSC veille à ce que les espaces de données s'appuient sur des pratiques communes et exploitent des composants standardisés, appelés « éléments constitutifs ». Ces éléments incluent notamment des outils partagés, tels que des solutions logicielles et des services spécifiques, qui permettent de garantir une mise en œuvre cohérente et adaptée aux besoins des utilisateurs. Ainsi, grâce à cette approche mutualisée, le DSSC favorise l'émergence d'un écosystème de données robuste et efficient, où chaque espace peut tirer parti des ressources existantes pour gagner en efficacité et en stabilité.

Avec l'entrée en vigueur de la nouvelle législation sur les données [957] et la mise en place de plusieurs initiatives européennes en matière d'espaces de données, la phase de mise en œuvre est désormais lancée. Durant cette étape, l'interopérabilité jouera un rôle central dans l'exploitation optimale du potentiel offert par ces espaces. Les normes constituent un levier essentiel pour favoriser cette interopérabilité, et leur utilité dépasse largement le simple cadre du partage de données électroniques. Dans d'autres domaines, comme les transactions commerciales, des standards bien établis facilitent déjà des processus, tels que la commande et la facturation électroniques, le partage de

---

953 RÈGLEMENT D'EXÉCUTION (UE) 2023/138 de la Commission du 21 décembre 2022 établissant une liste d'ensembles de données de forte valeur spécifiques et les modalités de leur publication et de leur réutilisation (Texte présentant de l'intérêt pour l'EEE).

954 L'annexe I de la directive (UE) 2019/1024 décline les ensembles de données de forte valeur en six catégories thématiques: 1) géospatiales; 2) observation de la terre et environnement; 3) météorologiques; 4) statistiques; 5) entreprises et propriété d'entreprises; et 6) mobilités.

955 https://dssc.eu/

956 https://digital-strategy.ec.europa.eu/en/activities/digital-programme

957 RÈGLEMENT (UE) 2023/2854 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données. (Texte présentant de l'intérêt pour l'EEE).

catalogues de produits ou encore les paiements numériques. Toutefois, dans l'économie des données, un changement fondamental s'opère : les données elles-mêmes deviennent l'objet de la transaction. Cette évolution entraîne l'émergence de nouveaux modèles économiques, de cadres réglementaires inédits et d'infrastructures adaptées, nécessitant l'élaboration de normes spécifiques pour garantir un fonctionnement efficace et sécuriser. Les politiques européennes en matière de données prennent en compte différents modes de partage de l'information. Si l'interopérabilité des données peut être intégrée au sein d'un espace de données, elle n'est pas pour autant une obligation. Il est donc crucial de définir des normes capables de s'adapter à une diversité de contextes, en accordant une attention particulière aux espaces de données européens communs, qui représentent l'un des piliers du marché unique des données. Dans cette optique, il est important de distinguer l'interopérabilité des espaces de données de celle des données elles-mêmes. Cette différenciation permettra d'identifier avec précision les types de normes requises et de mieux structurer les efforts visant à garantir une harmonisation efficace au sein de l'écosystème européen des données.

Grâce au nouveau cadre législatif (La Nouvelle Approche)[958], l'Union européenne dispose d'un outil particulièrement efficace pour renforcer la réglementation en s'appuyant sur des règles techniques précises, incarnées par les normes européennes harmonisées. Ce dispositif repose sur un principe fondamental : les textes réglementaires définissent avant tout les objectifs à atteindre, à travers des exigences essentielles qui doivent être respectées pour permettre la commercialisation d'un produit au sein du marché unique européen. Les normes européennes harmonisées jouent un rôle clé en traduisant ces exigences en solutions techniques concrètes. Lorsqu'une demande de normalisation est formulée par la Commission européenne, les organismes européens de normalisation coordonnent le travail des experts issus de diverses parties prenantes afin d'élaborer les normes requises. Lorsqu'un produit est soumis à une réglementation spécifique, il peut prouver sa conformité aux exigences essentielles en appliquant la norme harmonisée correspondante. Ce principe, connu sous le nom de présomption de conformité, s'est imposé comme l'un des mécanismes fondamentaux garantissant le bon fonctionnement du marché unique européen. Dans cette optique, le NLF constitue un pilier central de l'infrastructure européenne de qualité, qui englobe plusieurs domaines essentiels, tels que la métrologie, l'accréditation, la normalisation, l'évaluation de la conformité et la surveillance du marché. Bien qu'il soit possible de démontrer la conformité aux exigences essentielles par d'autres moyens, la présomption de conformité demeure l'approche la plus efficace et la plus largement adoptée. Dans ce contexte, le *Data Act* s'inscrit dans la logique du NLF. Son ambition est de structurer les exigences essentielles relatives à la gestion des données en s'appuyant sur un ensemble de normes européennes harmonisées. En intégrant ce cadre normatif, l'objectif est de faciliter le partage et l'utilisation des

[958] https://www.francenormalisation.fr/les-acteurs-de-la-normalisation/la-nouvelle-approche/

données dans un environnement fiable et conforme aux réglementations en vigueur, renforçant ainsi la sécurité juridique et la fluidité des échanges de données au sein de l'Union européenne.

Pour répondre à ces défis, plusieurs cadres de référence se sont déjà développés afin de structurer et d'harmoniser les pratiques dans ce domaine. Des organisations telles qu'IDSA[959], GAIA-X[960], FIWARE[961], MyData[962] et iShare[963] ont contribué à cet effort en définissant des spécifications techniques et en mettant à disposition des logiciels libres destinés à soutenir ces initiatives. Dans une démarche de convergence, ces différents acteurs ont uni leurs forces au sein du DSSC, avec l'ambition d'adopter une approche commune en matière de gestion des espaces de données. Toutefois, il reste à déterminer dans quelle mesure cette collaboration aboutira à une harmonisation effective des spécifications techniques ou si elle débouchera plutôt sur un modèle favorisant la coexistence de plusieurs approches complémentaires. Un exemple notable de ces initiatives est le protocole Dataspace développé par l'IDSA[964]. Conçu pour faciliter le partage de données de manière interopérable, ce protocole repose sur un cadre où les échanges sont régis par un contrôle d'utilisation strict et s'appuient sur des technologies Web. Il définit un ensemble de schémas et de protocoles permettant aux entités de

---

959 International Data Spaces Association (IDSA) est une association à but non lucratif fondée en 2016 par la Fraunhofer-Gesellschaft et établie à Dortmund, en Allemagne. L'IDSA regroupe plus de 150 organisations membres de 28 pays et développe des standards pour les espaces de données souverains, notamment le modèle d'architecture de référence IDS (IDS-RAM), le Rulebook IDSA et le Dataspace Protocol. Son objectif est de permettre aux organisations de partager des données tout en conservant un contrôle total sur leur utilisation. Voir : https://internationaldataspaces.org. Consulté le 18 décembre 2025.

960 GAIA-X : initiative européenne lancée en 2019 par la France et l'Allemagne visant à créer une infrastructure de données fédérée, sécurisée et souveraine. L'association internationale sans but lucratif GAIA-X AISBL (Association Internationale Sans But Lucratif), constituée à Bruxelles en 2020, développe un cadre de spécifications, de règles et de politiques pour favoriser l'émergence d'écosystèmes numériques décentralisés conformes aux valeurs européennes de transparence, d'ouverture et de protection des données. Voir : https://gaia-x.eu. Consulté le 18 décembre 2025.

961 FIWARE Foundation est une organisation à but non lucratif fondée en 2016, dont le siège est établi à Berlin. Elle promeut l'adoption de standards ouverts, implémentés via des technologies open source, pour faciliter le développement de solutions intelligentes dans des domaines tels que les villes intelligentes, l'énergie, l'agriculture et l'industrie. Parmi ses membres fondateurs figurent Atos, Engineering, NEC, Red Hat et Telefónica. FIWARE développe notamment le Context Broker Orion et le standard NGSI-LD, sélectionné par la Commission européenne comme brique de base du Connecting Europe Facility (CEF). Voir : https://www.fiware.org. Consulté le 18 décembre 2025.

962 MyData Global est une organisation internationale à but non lucratif basée à Helsinki (Finlande), qui promeut une approche centrée sur l'humain dans la gestion des données personnelles. Fondée sur la Déclaration MyData, l'organisation compte plus de 100 organisations membres et près de 400 membres individuels issus de plus de 40 pays sur six continents. Elle vise à donner aux individus le contrôle sur leurs données personnelles tout en permettant aux organisations de développer des services innovants dans le respect des droits numériques. Voir : https://mydata.org. Consulté le 18 décembre 2025.

963 iSHARE Foundation est une fondation internationale à but non lucratif établie aux Pays-Bas en 2018, responsable du développement et de la maintenance du iSHARE Trust Framework. Initialement conçu pour l'industrie logistique néerlandaise, ce cadre de confiance fournit des spécifications techniques standardisées pour l'identification, l'authentification et l'autorisation dans les espaces de données, permettant aux organisations de partager des données de manière sécurisée tout en conservant le contrôle de leurs droits. L'iSHARE Foundation collabore étroitement avec l'IDSA depuis 2019 et a cofondé l'Eclipse Dataspace Working Group en 2023. Voir : https://ishare.eu.

964 International Data Spaces Association (IDSA). Le Dataspace Protocol est un ensemble de spécifications conçues pour faciliter le partage interopérable de données entre entités régies par le contrôle d'usage et basées sur les technologies Web. Ces spécifications définissent les schémas et protocoles requis pour que les entités publient des données, négocient des accords et accèdent aux données dans le cadre d'une fédération de systèmes techniques appelée Dataspace. Voir : https://internationaldataspaces.org/idsa-is-standardizing-the-dataspace-protocol/

publier des données, d'établir des accords et d'accéder aux informations dans un écosystème fédéré, connu sous le nom de Dataspace. Ce protocole est en cours de développement, en parallèle d'autres travaux de normalisation menés par des organismes internationaux. Notamment, l'ISO/IEC JTC1/SC 38[965], qui se consacre aux infrastructures de cloud computing et aux plateformes distribuées, joue un rôle clé dans l'élaboration des standards techniques qui encadreront ces nouveaux environnements d'échange de données. Ces efforts de normalisation s'articulent autour de plusieurs normes clés visant à structurer et à encadrer le développement des espaces de données. Parmi elles, l'ISO/IEC DIS 20151[966], actuellement en cours d'élaboration, définira les principes fondamentaux ainsi que les caractéristiques essentielles qui régissent ces environnements. Cette norme fournira un cadre conceptuel permettant d'harmoniser les pratiques et d'assurer une compréhension commune des espaces de données. Parallèlement, l'ISO/IEC 19941[967], déjà publiée, se concentre sur deux aspects fondamentaux, l'interopérabilité et la portabilité. Ces éléments sont indispensables pour garantir des échanges fluides entre différents systèmes et assurer la mobilité des données sans dépendance excessive à une infrastructure spécifique. De plus, de nouveaux travaux ont été initiés pour approfondir des notions cruciales, telles que la souveraineté numérique et l'autonomie organisationnelle. Ces réflexions s'inscrivent dans le contexte plus large de l'informatique en nuage et des systèmes distribués, où il devient essentiel de garantir aux organisations un contrôle accru sur leurs données et infrastructures, tout en facilitant leur intégration dans un écosystème numérique globalisé.

Au sein de la communauté des villes intelligentes, un nouveau cadre d'interopérabilité a été introduit, il s'agit des Mécanismes d'Interopérabilité minimale (MIM). Ce concept vise à établir un socle commun de capacités pour les plateformes de gestion des données urbaines, garantissant ainsi un niveau d'interopérabilité suffisant pour permettre leur intégration fluide dans différents écosystèmes numériques. Les MIM jouent un rôle essentiel en instaurant des exigences fondamentales harmonisées, favorisant ainsi une adoption cohérente et réduisant les disparités entre les solutions technologiques. Leur mise en œuvre vise à améliorer la scalabilité, à encourager le partage des ressources et à assurer la

---

965 ISO/IEC JTC 1/SC 38 – Plate-formes et services d'applications distribuées. Le SC 38 fait office d'entité de réflexion, de promotion et d'intégration des systèmes portant sur l'informatique en nuage, les plates-formes distribuées, ainsi que l'application de ces technologies. Le SC 38 fournit des recommandations au JTC 1, à l'IEC, à l'ISO et à d'autres entités chargées de l'élaboration des normes dans les domaines précités. Voir : https://www.iso.org/fr/committee/601355/x/catalogue/p/0/u/1/w/0/d/0.

966 ISO/IEC DIS 20151 – Information technology — Cloud computing and distributed platforms — Dataspace concepts and characteristics. Cette norme vise à fournir les concepts fondamentaux et les caractéristiques essentielles des espaces de données (dataspaces). Elle établit un cadre conceptuel permettant d'harmoniser les pratiques et d'assurer une compréhension commune entre toutes les organisations impliquées dans le développement et l'utilisation d'espaces de données. La norme distingue clairement les espaces de données d'autres paradigmes informatiques tels que les data lakes, data warehouses, data fabrics ou data meshes. Voir : https://www.iso.org/standard/86589.html.

967 ISO/IEC 19941:2017 – Information technology — Cloud computing — Interoperability and portability.Cette norme spécifie les types d'interopérabilité et de portabilité dans le cloud computing, les relations et interactions entre ces deux aspects transversaux, ainsi que la terminologie commune et les concepts utilisés pour discuter de l'interopérabilité et de la portabilité, en particulier en ce qui concerne les services cloud. Voir : https://www.iso.org/standard/66639.html.

pérennité des systèmes. De plus, ils offrent une protection aux parties prenantes en limitant les risques liés à une dépendance excessive envers un fournisseur unique et en évitant des coûts élevés liés à des adaptations complexes de l'interopérabilité. Ces travaux de standardisation sont actuellement menés au sein de la Commission d'Étude 20 de l'UIT-T, qui se consacre aux Internet des objets (IoT) et aux villes et communautés intelligentes (SC&C)[968]. L'objectif est de structurer un cadre de référence permettant aux infrastructures urbaines de bénéficier d'une connectivité et d'une interopérabilité optimales, tout en assurant une intégration harmonieuse des nouvelles technologies au service des collectivités.

Le renforcement du cadre législatif européen, notamment à travers le règlement 1025/2012 imposant des exigences d'inclusivité, le Data Act établissant les principes de partage sécurisé, ou encore la Nouvelle Approche liant normes harmonisées et conformité réglementaire, confère à l'Union européenne des leviers d'action uniques. La présomption de conformité associée aux normes harmonisées, mécanisme central du marché unique, illustre comment l'Europe parvient à articuler souveraineté réglementaire et excellence technique normative. Cette capacité à faire converger cadres législatifs et standards techniques constitue un atout géopolitique majeur, permettant à l'Europe de défendre non seulement ses intérêts économiques immédiats, mais également sa vision d'une gouvernance numérique respectueuse des droits fondamentaux et de la souveraineté des acteurs. Toutefois, ces avancées stratégiques ne sauraient masquer une réalité préoccupante : les efforts européens pour renforcer sa participation et son influence dans la normalisation internationale se déploient dans un contexte global où les règles du jeu normatif elles-mêmes sont en train d'être redéfinies. Les transformations observées au sein du système européen, bien qu'essentielles, ne représentent qu'une facette d'une recomposition géopolitique plus profonde qui affecte l'ensemble de l'architecture mondiale de la normalisation. Car si l'Europe cherche à consolider sa position dans les instances internationales existantes, ces instances font face à des fractures structurelles qui menacent leur légitimité et leur capacité à produire des standards véritablement universels.

Les dynamiques de renforcement stratégique que nous venons d'analyser au niveau européen s'inscrivent en réalité dans un contexte de fragmentation croissante du système normatif mondial. Alors que la première partie de notre analyse s'est concentrée sur les réponses institutionnelles et techniques déployées par l'Union européenne pour maintenir son influence normative, il convient désormais d'élargir la focale pour examiner les fractures structurelles qui traversent l'ensemble de la gouvernance internationale des normes. Ces lignes de rupture géopolitiques, loin d'être de simples accidents conjoncturels, révèlent des tensions fondamentales quant à la nature même de la normalisation à l'ère numérique : qui peut participer effectivement à l'élaboration des standards mondiaux ? Selon quelles

[968] SG20: Internet of things (IoT) and smart cities and communities (SC&C). https://www.itu.int/en/ITU-T/studygroups/2025-2028/20/Pages/default.aspx

modalités d'accès ? Au service de quels intérêts et de quelles valeurs ? Et avec quelles conséquences pour la souveraineté technologique des États et des régions ?

2. Les nouvelles fractures géopolitiques dans la gouvernance des normes

L'histoire de la normalisation internationale se confond, depuis l'après-Seconde Guerre mondiale, avec celle de la mondialisation économique dont elle constitue l'un des rouages essentiels. La création de l'Organisation internationale de normalisation en 1947[969] s'inscrit dans le projet d'un ordre économique libéral visant à faciliter la reconstruction et l'expansion des échanges commerciaux par l'harmonisation des spécifications techniques. Durant les décennies qui ont suivi, la normalisation internationale a directement contribué à l'accélération des flux transfrontaliers, circulation des marchandises, mobilité des personnes, transmission des données, en établissant des référentiels communs permettant l'interopérabilité des systèmes productifs et l'intégration progressive des économies nationales dans des chaînes de valeur mondialisées. Toutefois, cette trajectoire d'ouverture et d'interconnexion croissante masque une réalité géographique profondément asymétrique. Ainsi, la participation aux processus normatifs internationaux demeure l'apanage d'un nombre restreint de territoires, dessinant une cartographie de l'influence technique où se superposent et se renforcent mutuellement les héritages coloniaux, les inégalités de développement et les rapports de domination économique contemporains.

Cette géographie inégalitaire de la normalisation se manifeste avec une acuité particulière au sein du Comité technique 211 de l'ISO, consacré aux informations géographiques et géomatique. L'absence quasi-totale du continent africain, la faible représentation de l'Amérique du Sud et l'invisibilisation relative de l'Asie occidentale dans les travaux de ce comité ne résultent pas d'un désintérêt de ces régions pour les enjeux normatifs, au contraire, les standards géospatiaux structurent de manière déterminante les infrastructures numériques, les politiques d'aménagement territorial et les stratégies de valorisation des ressources naturelles dans l'ensemble des pays du monde. Cette marginalisation révèle plutôt l'existence de barrières structurelles, financières, institutionnelles, cognitives, qui segmentent l'espace normatif mondial en zones d'influence différenciées, reproduisant à l'échelle des arènes techniques les clivages géopolitiques qui organisent l'économie internationale. Alors que l'Europe occidentale, l'Amérique du Nord et le Japon constituent depuis l'origine les centres de gravité normatifs, concentrant l'essentiel des secrétariats de comités techniques, des expertises mobilisées et des propositions de standards, d'immenses territoires demeurent relégués dans une

[969] Voir Première partie de cette thèse pour une analyse détaillée du contexte de création de l'ISO en 1947 et de son rôle dans la reconstruction de l'ordre économique international d'après-guerre.

position de récepteurs passifs de normes élaborées ailleurs, sans capacité effective d'influer sur des règles techniques qui affectent pourtant directement leurs économies et leurs souverainetés.

L'émergence, au cours des deux dernières décennies, de nouvelles puissances normatives asiatiques, (Chine, Corée du Sud, Inde) vient certes complexifier cette cartographie binaire opposant centres producteurs et périphéries consommatrices de normes. La stratégie chinoise, en particulier, illustre comment un État peut mobiliser des ressources massives pour transformer sa position dans la hiérarchie normative internationale. En effet, à travers le programme China Standards 2035, Beijing s'est fixé l'objectif explicite de devenir le principal exportateur de standards techniques mondiaux, investissant massivement dans la participation aux instances internationales, multipliant les propositions de normes dans les technologies émergentes (5G, intelligence artificielle, blockchain) et plaçant méthodiquement ses experts dans les positions de leadership des comités techniques[970]. Cette ascension normative chinoise ne se traduit pas par une démocratisation de l'accès aux processus de standardisation, mais plutôt par une recomposition oligopolistique où un nombre limité de puissances se disputent le contrôle des infrastructures techniques qui structureront l'économie numérique du XXIe siècle. Loin de réduire les fractures géographiques qui traversent l'espace normatif mondial, cette multipolarisation émergente pourrait au contraire les approfondir en créant de nouvelles zones d'exclusion pour les pays qui ne disposent ni des moyens de participer aux standards occidentaux, ni de la capacité de s'aligner sur les écosystèmes normatifs alternatifs portés par les puissances asiatiques.

Cette fragmentation géographique de la normalisation revêt une importance géopolitique considérable dans la mesure où les normes internationales, bien qu'adoptées formellement sur une base volontaire, exercent une contrainte de facto sur l'ensemble des acteurs économiques mondiaux. Les standards publiés par l'ISO servent de référence dans les accords commerciaux bilatéraux et multilatéraux, structurent les cahiers des charges des appels d'offres publics, conditionnent l'accès aux marchés d'exportation et déterminent les trajectoires technologiques des industries. Par ailleurs, les consortiums privés de normalisation, dont les conditions d'accès sont souvent plus restrictives encore que celles des organisations intergouvernementales, façonnent de manière croissante les standards techniques dominants dans les secteurs stratégiques du numérique, renforçant l'asymétrie entre acteurs économiques capables de participer à ces arènes exclusives et ceux qui en sont structurellement exclus[971]. Cette situation crée un paradoxe fondamental, alors même que la mondialisation économique

---

970 Asia Society Policy Institute (2021). "Stacking the Deck: China's Influence in International Technology Standards Setting", novembre 2021. Consulté le 20 décembre 2025. Le programme China Standards 2035 vise explicitement à *« accélérer la conversion des standards techniques avantageux de la Chine en standards internationaux »* et mobilise des ressources financières massives pour placer des experts chinois dans les positions de leadership des comités techniques internationaux.

971 Groupe d'Études Géopolitiques (2024). « L'Europe comme puissance normative internationale : état des lieux et perspectives ». L'article souligne que *« la participation dans les instances de normalisation technique devient un marqueur de la puissance normative »* et que les consortiums privés comme l'Open Geospatial Consortium (OGC)

a provoqué, pour reprendre les termes du professeur Jean-Bernard Auby, une *« spatialisation et déterritorialisation des activités et des mécanismes économiques et sociaux, une désétatisation des sociétés et du monde, ainsi qu'une croissance des réalités et des mécanismes transnationaux »*[972], l'architecture institutionnelle de la normalisation technique demeure profondément territorialisée, reflétant et perpétuant les hiérarchies géopolitiques héritées de l'ordre westphalien.

Face à ces asymétries structurelles, les organisations régionales émergent comme des instruments potentiels de rééquilibrage géopolitique dans le domaine normatif. L'Association des nations de l'Asie du Sud-Est (ASEAN), qui regroupe dix États d'Asie du Sud-Est[973], l'Union africaine (UA), organisation intergouvernementale rassemblant l'ensemble des pays du continent africain[974], ou encore le Marché commun du Sud (Mercosur), zone de libre-échange sud-américaine[975], constituent des structures de coordination régionale permettant théoriquement de mutualiser les ressources, d'harmoniser les positions et d'accroître le poids collectif de pays individuellement marginalisés dans les négociations normatives internationales. Ces regroupements régionaux offrent la possibilité d'une intégration normative par paliers, en favorisant notamment l'adoption coordonnée de standards internationaux à l'échelle de régions entières, ils peuvent créer des marchés suffisamment vastes pour que les normes ainsi harmonisées acquièrent une masse critique, incitant les acteurs économiques globaux à s'y conformer. Cette stratégie de régionalisation normative présente toutefois une certaine ambivalence, puisqu'elle peut fonctionner soit comme un tremplin vers l'intégration dans le système normatif global, permettant aux pays en développement d'acquérir progressivement les capacités techniques et institutionnelles nécessaires à une participation effective aux instances internationales, soit comme un mécanisme de subordination régionale, où l'adoption de standards élaborés ailleurs consolide la dépendance technologique et économique vis-à-vis des puissances normatives dominantes.

Cette tension entre intégration globale et fragmentation régionale s'inscrit dans un contexte géopolitique plus large marqué par la résurgence de logiques de blocs antagonistes. Le retour de politiques isolationnistes et protectionnistes aux États-Unis, l'invasion de l'Ukraine par la Russie et

---

imposent des barrières d'entrée financières et institutionnelles encore plus restrictives que l'ISO.

[972] Auby, Jean-Bernard (2003). La globalisation, le droit et l'État. Paris : Montchrestien, p. 14. Cité dans Collé Seck, Ami (2018). "Intégration et Souveraineté étatique, approche comparatives entre l'Europe et l'Afrique à travers l'UE, l'UEMOA et l'OHADA", thèse de doctorat en droit, Normandie Université, p. 3.

[973] L'Association des nations de l'Asie du Sud-Est (ASEAN) regroupe dix pays : Indonésie, Thaïlande, Malaisie, Brunei, Vietnam, Laos, Myanmar, Cambodge, Philippines et Singapour. La Papouasie-Nouvelle-Guinée et le Timor oriental sont membres observateurs. Créée en 1967, l'ASEAN constitue un espace économique de plus de 660 millions d'habitants représentant la cinquième économie mondiale.

[974] L'Union africaine (UA), créée le 9 juillet 2002 à Durban (Afrique du Sud) en application de la Déclaration de Syrte du 9 septembre 1999, a remplacé l'Organisation de l'unité africaine (OUA). Elle regroupe l'ensemble des pays du continent africain ainsi que Madagascar, soit 55 États membres représentant plus de 1,3 milliard d'habitants.

[975] Le Marché commun du Sud (Mercosur/Mercosul) est une zone de libre-échange regroupant l'Argentine, la Bolivie, le Brésil, le Paraguay et l'Uruguay. Le Venezuela est suspendu depuis décembre 2016. Le Chili, la Colombie, le Pérou et l'Équateur sont pays associés. Créé en 1991 par le Traité d'Asunción, le Mercosur représente un marché de plus de 290 millions d'habitants et constitue la quatrième zone économique intégrée au monde.

l'intensification des tensions sino-américaines ont révélé la fragilité du système multilatéral d'après-guerre et font peser le risque d'une reterritorialisation des échanges économiques selon des lignes de fracture idéologiques et sécuritaires. Comme le souligne Pierre-Olivier Gourinchas, conseiller économique du FMI, le monde fait face à une menace de *« fragmentation en blocs économiques distincts avec des disparités d'idéologies, de systèmes politiques, de normes technologiques, de systèmes de paiement et de commerce transfrontaliers »*[976]. Cette dynamique de balkanisation géoéconomique pourrait se traduire, dans le domaine de la normalisation, par l'émergence de sphères d'influence normatives concurrentes où différents ensembles géopolitiques développeraient des standards techniques incompatibles, reproduisant à l'échelle des infrastructures numériques et des protocoles de communication les divisions qui structurent désormais l'ordre international. L'hypothèse d'une fracturation de l'espace normatif en blocs régionaux antagonistes ne relève pas de la simple spéculation géopolitique. Des indices convergents suggèrent que cette recomposition territoriale est déjà en cours. À titre d'exemple, la Chine promeut activement ses propres standards dans les technologies de l'information à travers la Digital Silk Road, diffusant ses normes de gouvernance numérique dans les pays partenaires de l'initiative Belt and Road[977], l'Union européenne cherche à affirmer son autonomie stratégique en développant des standards alternatifs dans des domaines comme la protection des données (RGPD), l'intelligence artificielle éthique ou les espaces communs de données. Les États-Unis utilisent leur contrôle sur les infrastructures numériques mondiales et les consortiums privés de normalisation pour maintenir leur prééminence normative dans les technologies émergentes. Cette multipolarité normative conflictuelle transforme radicalement la nature même de la standardisation internationale : de mécanisme technique visant à faciliter l'interopérabilité globale, elle devient un terrain d'affrontement géopolitique où s'expriment des visions antagonistes de la gouvernance technologique, de la souveraineté numérique et de l'ordre économique mondial.

Dans ce contexte de recomposition géopolitique accélérée, un événement déstabilisateur majeur pourrait précipiter une fragmentation irréversible du système normatif international. L'effondrement de la confiance dans les institutions multilatérales, déjà fragilisées par les tensions géopolitiques actuelles, entraînerait mécaniquement un repli souverainiste où chaque État ou bloc régional chercherait à sécuriser son autonomie technologique en développant ses propres standards nationaux ou régionaux,

---

[976] Gourinchas, Pierre-Olivier, « Un casse-tête géoéconomique », *Finances & Développement*, FMI, juin 2022. L'auteur décrit *« un bouleversement soudain des plaques tectoniques géopolitiques qui révèle des failles cachées »* et met en garde contre une fragmentation mondiale en *« blocs économiques distincts avec des disparités d'idéologies, de systèmes politiques, de normes technologiques, de systèmes de paiement et de commerce transfrontaliers, et de monnaies de réserve. »*

[977] Miquel, Emma. « L'État de droit et la souveraineté numérique chinoise : une analyse de la stratégie de contrôle et d'extension de réseau numérique », *Questions constitutionnelles*. Revue de droit constitutionnel, 2025. [En ligne]. Disponible sur : https://questions-constitutionnelles.fr/letat-de-droit-et-la-souveraineté-numerique-chinoise-une-analyse-de-la-strategie-de-controle-et-dextension-de-reseau-numerique/. Consulté le 30 novembre 2025

quitte à sacrifier l'interopérabilité globale sur l'autel de la sécurité stratégique. Les règles de la normalisation internationale, telles qu'elles se sont cristallisées au cours des sept décennies d'existence de l'ISO, pourraient ainsi être bouleversées, laissant place à une mosaïque de référentiels techniques concurrents structurés selon des logiques d'alliances géopolitiques plutôt que de coopération technique. Face à cette possibilité de bifurcation normative, des stratégies d'acteurs se mettent d'ores et déjà en place, anticipant et parfois accélérant ce potentiel redécoupage de l'économie mondiale en sphères d'influence normatives distinctes.

C'est précisément cette triple fracture géopolitique (inégalités structurelles d'accès aux instances de normalisation, enjeux de souveraineté numérique dans les standards technologiques, recomposition des alliances stratégiques régionale), que la présente section se propose d'analyser systématiquement. En examinant successivement les obstacles qui maintiennent les pays en développement dans une position subalterne au sein du système normatif international, les dimensions territoriales et géopolitiques des standards géographiques dans un contexte de numérisation accélérée, puis les dynamiques de coopération et de compétition qui redessinent la carte des alliances normatives régionales, nous chercherons à comprendre comment ces fractures interconnectées transforment la gouvernance mondiale des normes techniques et quelles implications elles comportent pour la stabilité du système commercial multilatéral, la diffusion des innovations technologiques et l'équilibre géopolitique global. Cette analyse devra permettre également d'évaluer dans quelle mesure les réponses institutionnelles déployées par l'Union européenne peuvent contribuer à atténuer ces fractures ou risquent au contraire d'approfondir les lignes de division qui fragmentent l'espace normatif mondial.

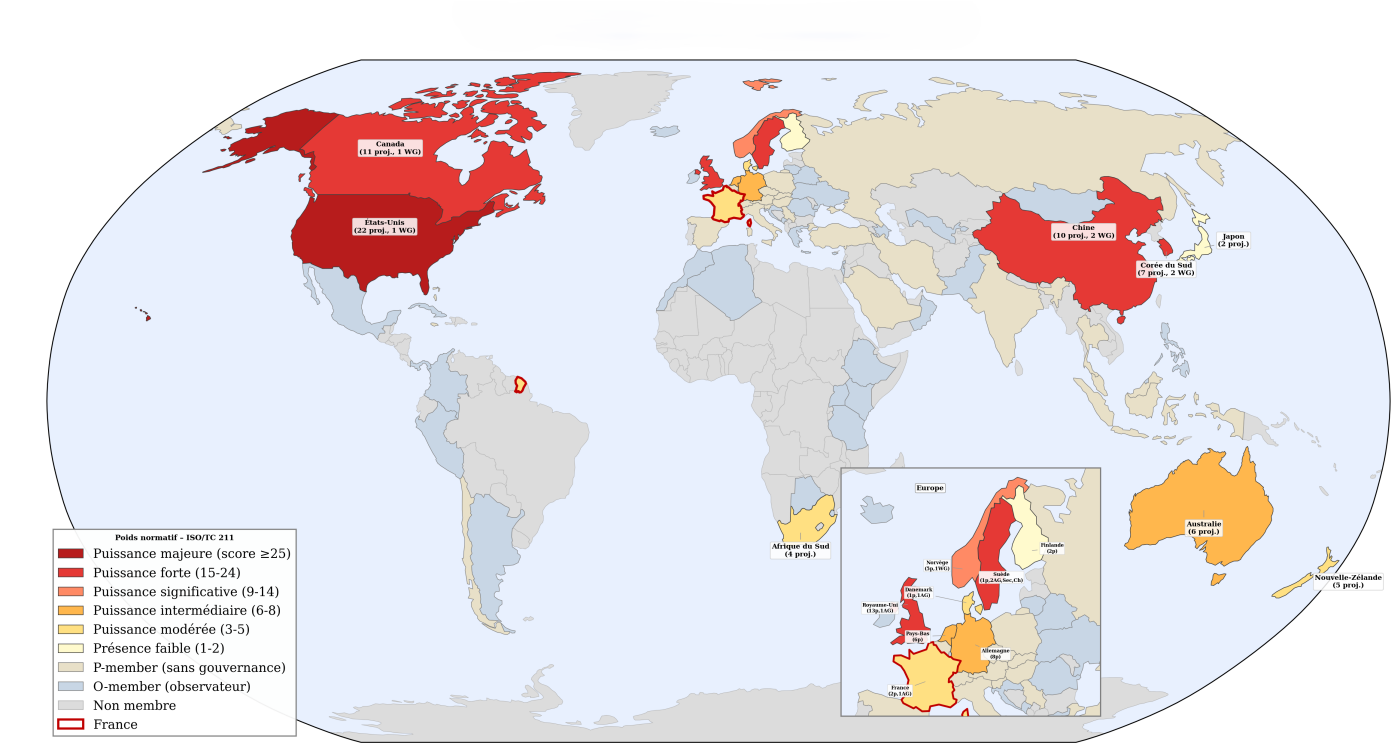
2.1. Inégalités d'accès aux instances de normalisation pour les pays en développement

La normalisation internationale représente un levier important pour favoriser les échanges commerciaux, en particulier pour les pays en développement. Dans le cadre de cette thèse consacrée à la géopolitique de la normalisation des données géographiques, les pays en développement sont définis, non pas selon les critères économiques classiques (PIB par habitant, IDH, taux d'alphabétisation), mais à travers le prisme de leur position structurelle dans l'architecture mondiale de la gouvernance normative. Cette approche géopolitique permet de dépasser les catégorisations binaires traditionnelles (Nord/Sud, développés/sous-développés) qui, comme l'a souligné la Banque mondiale en 2016, sont devenues « obsolètes » face à l'hétérogénéité croissante des trajectoires de développement nationales[978]. Sont ainsi considérés comme pays en développement l'ensemble des États présentant une capacité limitée d'influence dans les processus de normalisation internationale. Cette limitation résultant d'une combinaison de facteurs, marginalisation institutionnelle dans les comités techniques de l'ISO, de la CEI et de l'UIT, déficit de capacités techniques et organisationnelles, contraintes économiques rendant prohibitive la participation régulière aux instances internationales, et héritage colonial perpétuant des relations de dépendance technologique (cf. carte 8)[979].

[978] Banque mondiale, World Development Indicators 2016, Washington DC, 2016. Dans l'édition 2016 de ses indicateurs de développement, la Banque mondiale a renoncé pour la première fois à distinguer « pays en développement » et « pays développés », une catégorisation devenue « obsolète » selon l'institution face à l'hétérogénéité croissante des situations nationales.

[979] Le système de classement utilisé pour classer les pays dans la carte 8 a été établi par l'auteur : le score est obtenu en additionnant les responsabilités prises par les pays au sein de la gouvernance de l'ISO/TC 211, qu'il s'agisse des groupes de travail présidés, des projets dirigés ou des rôles occupés au sein des comités de liaison. (Projets dirigés x1) + (secrétariat de WG/JWG x5) + (Secrétariat d'AG x3) + (secrétariat TC x8) + (présidence TC x6).

Carte 8: Le poids normatif des nations au sein de l'ISO/TC 211 (2024)



Source : ISO/TC 211, recherches de l'auteur (2024)

Pour les pays en développement, l'accès aux instances où s'élaborent les normes techniques, et plus encore la capacité d'y exercer une influence effective, demeure un défi structurel qui perpétue leur marginalisation dans la gouvernance économique mondiale et les place dans une situation de dépendance normative vis-à-vis des puissances dominantes. Cette situation revêt une dimension particulièrement critique dans le domaine des données géographiques numériques. Les standards techniques qui régissent la collecte, le traitement, l'échange et la visualisation de l'information géospatiale conditionnent en effet l'intégration aux chaînes de valeur mondiales, l'accès aux technologies satellitaires et de positionnement, et la maîtrise des infrastructures de données spatiales nationales. Comme le souligne la Conférence des Nations unies sur le commerce et le développement (CNUCED), les pays en développement ont besoin d'un soutien accru pour faire face aux nouvelles

normes mondiales[980], ce qui témoigne de l'ampleur du défi auquel ils sont confrontés dans un contexte où les données géographiques deviennent un actif stratégique de première importance.

Toutefois, les retombées positives de cette normalisation dépendent largement de la capacité de ces pays à mettre en œuvre les normes internationales en vigueur. Cette capacité d'adoption et d'application est elle-même étroitement liée à la manière dont les normes sont conçues, c'est-à-dire à leur adéquation avec les spécificités économiques, sociales, techniques et institutionnelles des pays en développement. La participation active de ces pays à l'élaboration des normes internationales est donc un enjeu crucial. Bien que l'on ait observé une augmentation de cette participation au fil du temps, notamment à la suite de l'entrée en vigueur des accords sur les mesures sanitaires et phytosanitaires (SPS)[981] et sur les obstacles techniques au commerce (OTC)[982], cette implication demeure généralement en deçà de celle des pays industrialisés. Autrement dit, même si les pays en développement sont aujourd'hui davantage représentés dans les processus de normalisation qu'ils ne l'étaient auparavant, leur contribution effective aux décisions reste limitée en comparaison avec celle des pays développés. Ce déséquilibre structurel a pour conséquence directe que les normes adoptées à l'échelle internationale reflètent encore majoritairement les intérêts, les priorités et les capacités des économies les plus avancées, au détriment des réalités propres aux pays à plus faibles revenus. Dans ce contexte, la capacité institutionnelle et technique des pays en développement à participer aux travaux des organisations internationales de normalisation apparaît comme un facteur déterminant. Cette participation peut prendre des formes diverses et se situer à différents niveaux du processus normatif, chacun ayant une influence variable sur les résultats finaux. Il convient de souligner que de nombreux pays en développement sont formellement membres d'organismes internationaux de normalisation ainsi, en 2022, 75 % des États membres de l'Organisation internationale de normalisation (ISO) relevaient de cette catégorie [983]. Toutefois, leur rôle concret dans les activités centrales des comités techniques, qui sont les lieux stratégiques où les normes sont effectivement discutées et rédigées, ainsi que dans les instances décisionnelles ou administratives, reste souvent marginal, faute de ressources humaines, financières ou techniques suffisantes. Ainsi, l'influence des pays en développement sur le contenu des normes internationales demeure limitée, malgré une représentation croissante en termes de nombre. Cette situation remet en question la capacité du système international de normalisation à produire des normes véritablement inclusives et représentatives de la diversité des contextes

---

980 CONFÉRENCE DES NATIONS UNIES SUR LE COMMERCE ET LE DÉVELOPPEMENT (CNUCED). Rapport sur l'économie numérique 2024, Genève, Nations Unies, 2024. Disponible sur : https://unctad.org/

981 OMC, « Accord sur l'application des mesures sanitaires et phytosanitaires (Accord SPS) », Division du commerce et de l'environnement, 1er janvier 1995. https://www.wto.org/french/tratop_f/sps_f/spsagr_f.htm. Consulté le 21 février 2025.

982 OMC, « Série des Accords de l'OMC Obstacles techniques au commerce », Division du commerce et de l'environnement, 1er janvier 1995. https://www.wto.org/french/res_f/booksp_f/tbt3rd_f.pdf. Consulté le 21 février 2025.

983 ISO, « ISO's Action Plan for developing countries 2021-2025 Designed with members, for members. », 10 mai 2021. https://www.iso.org/news/ref2667.html. Consulté le 10 novembre 2022.

économiques mondiaux. Pour que les normes internationales puissent réellement soutenir le développement économique et l'intégration des pays en développement dans les échanges mondiaux, il est impératif que leur voix soit non seulement entendue, mais aussi pleinement prise en compte à toutes les étapes du processus normatif.

Les organisations internationales œuvrant dans le domaine de la normalisation ne forment pas un ensemble homogène. Elles présentent des différences marquées en ce qui concerne leur mandat institutionnel, leur architecture organisationnelle et les modalités de leur fonctionnement. Certaines de ces entités sont constituées comme des organisations intergouvernementales officielles, souvent rattachées à des institutions onusiennes, à l'instar du Comité d'experts des Nations Unies pour la gestion de l'information géospatiale à l'échelle mondiale (UN GGIM), qui traitent des données géographiques [984]. D'autres, telles que l'ISO ou la Commission électrotechnique internationale (CEI), se présentent comme des structures autonomes, généralement non gouvernementales, et souvent orientées vers la défense des intérêts du secteur industriel. Les différences institutionnelles entre ces diverses organisations influencent directement le degré d'implication des pays en développement. De manière générale, ceux-ci tendent à être davantage représentés dans les organismes de nature intergouvernementale. C'est le cas, par exemple, du Codex Alimentarius[985] et de l'Organisation mondiale de la santé animale (OMSA, ex-OIE)[986], qui bénéficie d'une forte participation des pays en développement. Ces deux structures ont pour mission explicite de protéger la santé publique, celle des consommateurs pour le Codex, et celle des animaux pour l'OIE, et leur statut intergouvernemental favorise une inclusion plus large des États, indépendamment de leur niveau de développement. À l'inverse, la participation des pays en développement dans des entités telles que la CEI demeure très

---

984 Le Comité d'experts des Nations unies sur la gestion de l'information géospatiale mondiale (UN GGIM) est l'un des neuf groupes d'experts du Conseil économique et social des Nations unies (ECOSOC) et visant à favoriser le développement mondial de l'information géospatiale. Source : https://fr.wikipedia.org/wiki/Comit%C3%A9_d'experts_des_Nations_unies_sur_la_gestion_mondiale_de_l'information_g%C3%A9ospatiale.

985 Le codex Alimentarius (ou codex alimentaire) est un programme commun de l'Organisation des Nations unies pour l'alimentation et l'agriculture (FAO) et de l'Organisation mondiale de la santé (OMS) consistant en un recueil de normes, codes d'usage, directives et autres recommandations relatifs à la production et à la transformation agroalimentaires qui ont pour objet la sécurité sanitaire des aliments, soit la protection des consommateurs et des travailleurs des filières alimentaires, et la préservation de l'environnement. Source : https://fr.wikipedia.org/wiki/Codex_Alimentarius.

986 L'Organisation mondiale de la santé animale (OMSA), anciennement Office international des épizooties (OIE), est une organisation intergouvernementale fondée en 1924, chargée d'améliorer la santé et le bien-être animal dans le monde. L'OMSA participe à la diffusion de normes internationales en matière vétérinaire afin de prévenir les épidémies. Elle compte 184 pays dans le monde. Source : Site officiel de l'OMSA. https://www.woah.org/fr/qui-nous-sommes/membres/. Les pays en développement représentent actuellement 81 % des membres du Codex, dont 60 % sont des pays à revenu faible ou moyen inférieur. En outre, la part des pays en développement a augmenté au fil du temps, tandis que celle des pays de l'OCDE à revenu élevé a diminué. Preibisch Kerry, Hension Spencer et Masakure Oliver, « Review of Developing Country Needs and Involvement in International Standards-Setting Bodies », Centre for Food Economics Research Department of Agricultural and Food Economics, The University of Reading, pp. 145, mars 2001, p. 50. https://www.researchgate.net/publication/228381418_Review_of_Developing_Country_Needs_and_Involvement_in_International_Standards-Setting_Bodies.

restreinte, ce qui reflète en partie les exigences d'adhésion et les ressources nécessaires pour prendre part activement à leurs travaux [987]. La situation est similaire pour l'ISO, au sein de laquelle seule une fraction minoritaire des pays en développement détient le statut de membre à part entière, limitant ainsi leur influence sur les processus de normalisation [988]. Ces dynamiques mettent en lumière une réalité préoccupante, qui est que la diversité des structures organisationnelles dans le système international de normalisation engendre des formes d'exclusion indirecte pour les pays aux capacités limitées. Cette inégalité d'accès et de représentation compromet leur possibilité de faire entendre leurs intérêts, et de veiller à ce que les normes techniques élaborées à l'échelle mondiale tiennent compte de leurs réalités économiques et sociales.

Les pays en développement font face à un ensemble de contraintes systémiques qui freinent leur engagement au sein des organisations internationales de normalisation. Ces obstacles sont étroitement liés à leur niveau global de développement, tant sur le plan économique que technologique[989], mais ils trouvent également leur origine dans les spécificités structurelles et institutionnelles des organismes de normalisation eux-mêmes qui ont été conçus par et pour les pays industrialisés. Parmi ces obstacles figurent en premier lieu les coûts financiers directement associés à la participation. Il s'agit notamment des cotisations exigées pour l'adhésion ou la pleine participation aux instances décisionnelles, ainsi que des frais liés aux déplacements internationaux et à l'hébergement lors des réunions techniques ou administratives. Pour de nombreux pays disposant de budgets restreints, ces dépenses représentent un frein important à une implication régulière et soutenue. Au-delà de ces considérations financières, les contraintes sont également d'ordre technique et humain. La disponibilité limitée de ressources qualifiées, qu'il s'agisse d'expertise scientifique, de compétences techniques ou de personnel formé aux enjeux de la normalisation, constitue un facteur de blocage majeur. Dans plusieurs contextes nationaux, les capacités internes à suivre, analyser et contribuer aux travaux normatifs internationaux restent faibles, en raison d'un manque de formation, d'institutions de soutien insuffisamment développées, ou encore de difficultés de coordination entre les acteurs concernés (secteurs public, privé

---

987 Les pays à haut revenu représentent 50 % des membres à part entière. Les pays à faible revenu ne représentent que 8 % (4 pays) des membres à part entière. En outre, les pays à faible revenu qui sont membres à part entière de la CEI sont des pays à la population très importante : l'Inde, le Pakistan, l'Indonésie et l'Ukraine. Source : Preibisch Kerry, Hension Spencer et Masakure Oliver, « Review of Developing Country Needs and Involvement in International Standards-Setting Bodies », Centre for Food Economics Research Department of Agricultural and Food Economics, The University of Reading, pp. 145, mars 2001, p. 47. https://www.researchgate.net/publication/228381418_Review_of_Developing_Country_Needs_and_Involvement_in_International_Standards-Setting_Bodies.

988 Dans l'ensemble, les pays en développement représentent 69 % des organismes membres de l'ISO. Ainsi, bien qu'une plus grande proportion de pays en développement membres aient le statut d'abonné ou de correspondant que les pays membres à revenu élevé, ils restent majoritaires au sein de l'ISO.

989 UN Trade and development, « Developing countries need more support to cope with new global sustainability reporting standards », 24 novembre 2021. Consulté le 30/03/2025 à : https://unctad.org/news/developing-countries-need-more-support-cope-new-global-sustainability-reporting-standards

et académique). Les structures et procédures administratives en vigueur, tant au sein des pays en développement qu'au sein des organisations de normalisation elles-mêmes, peuvent également représenter des entraves supplémentaires. Des processus décisionnels complexes, un accès limité à l'information, ou encore une absence de mécanismes clairs pour assurer une représentation nationale cohérente peuvent nuire à l'efficacité de la participation.

À cela s'ajoutent parfois des obstacles d'ordre plus subjectif, comme des perceptions négatives vis-à-vis des instances internationales, ou une forme de résignation face à un système perçu comme dominé par les intérêts des pays industrialisés. Ainsi, malgré la présence d'un grand nombre de ses experts dans les comités techniques de l'ISO, la Chine a mis du temps avant de voir ses propositions acceptées au sein des instances internationales de normalisation [990]. Les représentants des pays en développement font souvent face à des préjugés de la part des nations mieux implantées dans le système, du fait de l'« inexpérience supposée » de leurs experts[991]. Cette présomption d'incompétence, rarement formulée explicitement, mais opérant de manière diffuse dans les interactions quotidiennes des comités techniques, constitue une barrière invisible, mais puissante à la participation effective. Ainsi, une étude publiée dans la revue Research Policy en 2023 a démontré ce phénomène dans le domaine des technologies de l'information et de la communication. Les chercheurs Lennart Schott et Kerstin J. Schaefer ont analysé l'acceptation des contributions technologiques des « nouveaux venus » (latecomers) dans les processus de normalisation internationale, montrant qu'elle est significativement influencée par leur origine géographique, leur expérience antérieure et leurs réseaux de collaboration[992]. À qualité technique égale, une proposition émanant d'un expert d'un pays du Nord bénéficie d'une présomption de légitimité dont ne jouit pas son homologue du Sud. Ce biais systémique, qu'il soit conscient ou non, contribue à perpétuer la domination des pays industrialisés sur les processus normatifs.

Au-delà du « fossé numérique » entre pays en développement et pays développés, les pays en développement font face à un « fossé géospatial » spécifique qui aggrave leur marginalisation dans les processus de normalisation de l'information géographique. Ce fossé se manifeste à plusieurs niveaux, absences ou obsolescences des données cartographiques de base (réseaux géodésiques, modèles numériques de terrain, couverture d'imagerie satellitaire), faiblesse des infrastructures de données

---

990 Schott Lennart, et Schaefer Kerstin J., « Acceptance of Chinese latecomers' technological contributions in international ICT standardization — The role of origin, experience and collaboration », Research Policy, (52), janvier 2023. Consulté le 31/03/2025 sur : https://www.researchgate.net/publication/364639953_Acceptance_of_Chinese_latecomers'_technological_contributions_in_international_ICT_standardization_-_The_role_of_origin_experience_and_collaboration

991 Schott Lennart et Schaefer Kerstin J., « Acceptance of Chinese latecomers' technological contributions in international ICT standardization - The role of origin, experience and collaboration », Research Policy, (52), janvier 2023. https://www.researchgate.net/publication/364639953. Consulté le 22 décembre 2025.

992 Ibid.

spatiales nationales, pénurie de logiciels et d'équipements adaptés, ou encore manque de personnel qualifié. Comme le souligne un article de référence publié dans le journal Geo-spatial Information Science, « *bien que l'information géospatiale soit de plus en plus utilisée en Afrique et dans d'autres régions en développement, de nombreux pays sont frustrés par un accès limité aux données et l'absence d'outils permettant l'analyse et la visualisation. Le manque de cartographie de base cohérente et à jour — ensembles de données géographiques fondamentales telles que le contrôle géodésique, l'élévation, le drainage, les transports, l'occupation du sol, les noms géographiques, le régime foncier, etc. — à travers l'Afrique demeure un défi, bien que certains pays progressent individuellement* »[993]. Cette situation crée un cercle vicieux où les pays qui ne disposent pas de données géospatiales de qualité peinent à former des experts capables de contribuer aux travaux de normalisation. Leur absence des comités techniques fait que les normes élaborées ne tiennent pas suffisamment compte de leurs contraintes spécifiques, rendant leur mise en œuvre encore plus difficile. Les normes ISO 19100, par exemple, présupposent souvent l'existence d'infrastructures de données spatiales avancées (services web géospatiaux, catalogues de métadonnées, registres de référentiels) que la plupart des pays africains ne possèdent pas encore. Ainsi, le directeur du Centre africain de statistiques de la Commission économique pour l'Afrique, Oliver Chinganya, reconnaissait en 2023 que « *l'Afrique est encore confrontée au manque d'infrastructures et de personnel qualifié pour exploiter adéquatement la technologie géospatiale* »[994]. Cette carence en capacités techniques se traduit mécaniquement par une faible participation aux instances où se définissent les standards, perpétuant ainsi l'inadéquation entre les normes internationales et les réalités des pays africains.

Conscientes des obstacles rencontrés par les pays en développement pour s'impliquer pleinement dans les processus de normalisation internationale, plusieurs organisations compétentes en la matière ont mis en place divers mécanismes destinés à encourager et à soutenir leur participation. Ces efforts se traduisent par un éventail d'initiatives visant à atténuer les contraintes économiques, techniques et structurelles identifiées précédemment. Parmi les mesures adoptées, on peut citer la mise en place de systèmes de cotisation différenciée, ajustés en fonction du niveau de revenu national, permettant ainsi aux pays disposant de ressources économiques limitées de bénéficier d'un accès plus abordable aux structures décisionnelles. À cela s'ajoutent des dispositifs d'appui financier spécifiques, tels que des fonds destinés à couvrir les frais de déplacement et de séjour des représentants des pays en développement lors des réunions internationales. En parallèle, un certain nombre d'initiatives visent à

---

[993] Scott Greg et Rajabifard Abbas, « Sustainable development and geospatial information: a strategic framework for integrating a global policy agenda into national geospatial capabilities », *Geo-spatial Information Science*, vol. 20, n° 2, 2017. https://www.tandfonline.com/doi/full/10.1080/10095020.2017.1325594. Consulté le 2 octobre 2025.

[994] United Nations Economic Commission for Africa, « Africa must harness geospatial technology for sustainable development », 10 octobre 2023. https://www.uneca.org/stories/africa-must-harness-geospatial-technology-for-sustainable-development. Consulté le 18 novembre 2025.

renforcer les capacités techniques et logistiques de ces pays. Cela inclut l'assistance technique fournie pour améliorer la compréhension et l'application des normes, l'organisation de formations spécialisées, ainsi que la facilitation de la participation à distance, notamment par le biais du vote électronique ou postal. Des normes sont également proposées à des tarifs préférentiels afin de garantir un accès plus large à ces dernières. De plus, des dispositifs institutionnels ont été mis en place pour mieux représenter les intérêts spécifiques des pays en développement au sein des structures normatives internationales, comme le Comité pour les questions relatives aux pays en développement (DEVCO) au sein de l'ISO. Malgré la diversité et la pertinence de ces mesures, leur impact sur le niveau global de participation demeure limité. Bien que ces initiatives aient sans doute permis de lever certaines barrières, la représentation effective des pays en développement dans les processus centraux de normalisation reste, dans l'ensemble, relativement faible. Ce constat souligne la nécessité de renforcer ces mécanismes de soutien, mais aussi de repenser certaines modalités structurelles de la gouvernance normative afin de favoriser une inclusion plus équitable et durable.

L'établissement du Centre mondial de connaissances et d'innovation géospatiales des Nations unies (UN-GGKIC) à Deqing, dans la province chinoise du Zhejiang, en 2023, illustre les tentatives de rééquilibrage en cours, tout en soulevant des questions sur les rapports de force qui les sous-tendent. Inauguré après plusieurs années de négociation entre la Chine et le Secrétariat des Nations unies, ce centre a pour mission officielle de *« renforcer et faire progresser les capacités de développement en matière de gestion de l'information géospatiale des États membres, en particulier des pays en développement, et de renforcer le partage des connaissances et la coopération innovante »*[995]. Le choix d'implanter ce centre en Chine plutôt qu'en Europe ou en Amérique du Nord, où se trouvent la plupart des autres centres onusiens liés aux statistiques et aux données, témoigne de la reconnaissance du rôle croissant de Beijing dans la gouvernance mondiale de l'information géospatiale. Il soulève toutefois des interrogations sur l'influence que la Chine pourrait exercer sur les orientations du centre et sur les standards qu'il promeut auprès des pays en développement. Le financement important apporté par le gouvernement chinois (infrastructures, personnel, budget de fonctionnement) crée une relation de dépendance qui n'est pas sans rappeler les dynamiques à l'œuvre dans les projets de la BRI. Le Comité consultatif international (IAC) du centre, composé de 23 experts géospatiaux internationaux, présente une composition géographique plus équilibrée que les instances techniques traditionnelles. Il comprend notamment des co-présidents issus d'Afrique du Sud (Mme Maroale Chauke, Ministère de

[995] UN-GGIM Decision 12/101, établissement du Centre mondial de connaissances et d'innovation géospatiales des Nations unies (UN-GGKIC) à Deqing, Chine. https://ggim.un.org/meetings/2024/2024_Meeting_UN_GGKIC_IAC/. Consulté le 30 septembre 2025.

l'Agriculture) et d'Indonésie (M. Antonius Wijanarto, Agence d'information géospatiale)[996]. Lors de sa première année de fonctionnement, le UN-GGKIC a organisé des ateliers de renforcement des capacités au Cap (Afrique du Sud, août 2023), à Addis-Abeba (Éthiopie, octobre 2023), à Bali (Indonésie, novembre 2023), à Antigua-et-Barbuda (mai 2024) et aux Fidji (novembre 2024), ciblant en priorité les petits États insulaires en développement (PEID) et les pays les moins avancés (PMA)[997]. En mars 2024, une consultation d'experts et un atelier sur l'UN-IGIF ont été organisés à Maputo (Mozambique) en collaboration avec la SDG Data Alliance et la Commission économique pour l'Afrique[998].

Ces activités témoignent d'un effort réel pour aller vers les pays en développement et répondre à leurs besoins spécifiques. Reste à voir si le centre parviendra à maintenir son indépendance vis-à-vis de son pays hôte et à promouvoir des standards véritablement ouverts et interopérables, plutôt que de servir de vecteur à la diffusion des normes chinoises sous couvert de coopération onusienne.

Favoriser une participation accrue des pays en développement, et plus particulièrement des petits États et des pays les moins avancés, au sein des organisations internationales de normalisation constitue un enjeu de premier ordre. Répondre à cet objectif implique de surmonter un ensemble de défis complexes, qui relèvent à la fois de contraintes structurelles internes aux pays concernés et de facteurs systémiques propres à l'environnement institutionnel international. Un premier défi réside dans les ressources mobilisables par ces pays pour assurer une présence active et continue dans les instances de normalisation. Les coûts afférents à une participation soutenue, qu'ils soient financiers, humains ou logistiques, représentent un obstacle significatif, notamment pour les États disposant de budgets limités et de capacités institutionnelles réduites. Sans mécanismes d'appui adéquats, ces pays peinent à maintenir une implication régulière dans les travaux techniques, à suivre les évolutions normatives ou à faire valoir leurs positions. Un second défi concerne la capacité réelle de ces pays à s'impliquer de manière substantielle dans les processus décisionnels des organisations de normalisation. Cette capacité repose sur plusieurs facteurs interdépendants: la disponibilité d'expertise technique, la présence d'un cadre institutionnel permettant de coordonner efficacement la participation nationale, ainsi que l'existence de politiques publiques valorisant la normalisation comme levier de développement. En l'absence de ces éléments, la participation des pays en développement risque de rester symbolique, sans véritable influence sur les orientations normatives adoptées. Enfin, un troisième aspect, souvent sous-

---

996 « United Nations Global Geospatial Knowledge and Innovation Centre Report », Background document, UN-GGIM 14th Session, 2024. https://ggim.un.org/meetings/GGIM-committee/14th-Session/documents/. Consulté le 30 septembre 2025.

997 2025 Meeting of the International Advisory Committee (IAC) of the UN-GGKIC », Concept Note, 17 avril 2025. https://ggim.un.org/meetings/2025/2025_Meeting_UN_GGKIC_IAC/. Consulté le 3 octobre 2025.

998 « Implementing geospatial strategies », Expert consultation and workshop, Maputo, Mozambique, 24-28 mars 2024. https://ggim.un.org/meetings/2025/Maputo/. Consulté le 3 octobre 2025.

estimé, touche à la perception qu'ont les autres membres des organisations internationales de normalisation, en particulier les représentants des pays développés, des besoins, contraintes et capacités spécifiques des pays en développement. Une meilleure compréhension de ces réalités, de même qu'une reconnaissance explicite des avantages liés à une représentation plus équitable, est indispensable pour favoriser une approche inclusive de la normalisation. Une telle reconnaissance permettrait non seulement d'ajuster les mécanismes de participation existants, mais aussi d'encourager un partage plus équilibré du pouvoir décisionnel au sein des instances normatives. Ainsi, relever le défi de l'inclusion des pays en développement dans le système international de normalisation suppose une action conjointe, combinant soutien ciblé, renforcement des capacités internes et évolution des mentalités au sein des organisations elles-mêmes.

Divers leviers peuvent être envisagés pour favoriser une participation plus active et plus équitable des pays en développement au sein des organisations internationales de normalisation. Ces mécanismes, bien que multiples, ne sauraient être appliqués uniformément à l'ensemble des instances normatives, car leur pertinence et leur efficacité dépendent étroitement des spécificités institutionnelles, techniques et opérationnelles propres à chaque organisation. Parmi les dispositifs les plus souvent évoqués figure l'octroi d'un soutien financier ciblé, notamment pour permettre aux représentants des pays en développement de prendre part aux réunions internationales, dont la fréquence, le lieu et les coûts peuvent constituer des freins importants à l'engagement durable. À cela s'ajoute l'assistance technique, sous différentes formes, telles que le mentorat, le transfert de compétences ou les échanges de secrétariats entre les pays développés et les pays en développement, ce qui contribue à un renforcement progressif des capacités institutionnelles et humaines de ces derniers. Au-delà de ces formes d'appui direct, des réformes structurelles plus profondes pourraient également être envisagées. Celles-ci concerneraient à la fois l'organisation interne et les modes de gouvernance des institutions de normalisation internationales, dans le but de les rendre plus inclusives et représentatives, ainsi que les dispositifs administratifs des pays en développement eux-mêmes, afin de renforcer leur aptitude à organiser, coordonner et défendre leurs positions dans les arènes normatives internationales. Par ailleurs, l'amélioration du dialogue entre les pays développés et ceux en développement apparaît comme un levier transversal essentiel. Une meilleure compréhension mutuelle des intérêts, des contraintes et des objectifs stratégiques de chaque groupe de pays permettrait de créer un environnement plus propice à la coopération constructive et à la recherche de compromis équilibrés dans l'élaboration des normes. En complément, le renforcement de la coopération régionale entre pays en développement pourrait également jouer un rôle déterminant, en permettant la mutualisation des ressources, la coordination des positions et la création d'un front commun plus audible à l'échelle internationale. Cependant, l'élaboration d'une stratégie unique, applicable indistinctement à l'ensemble

des organisations internationales de normalisation, apparaît peu réaliste. La diversité des mandats, des structures organisationnelles, des modes de financement et des domaines de compétence des différentes instances rend nécessaire une approche différenciée et contextuelle. Toute initiative visant à accroître la participation des pays en développement doit ainsi être conçue sur mesure, en tenant compte des particularités de chaque organisation, des dynamiques régionales, et des priorités propres aux pays concernés.

Dans un contexte de mondialisation accrue et d'exigences qualitatives élevées sur les marchés internationaux, la question des normes techniques est devenue centrale pour les pays en développement. Ceux-ci doivent faire face à une double pression, garantir la qualité et la sécurité des produits sur leur marché domestique, et satisfaire aux critères d'accès imposés par les pays industrialisés. Si l'adoption unilatérale des standards internationaux constitue une voie possible, elle s'avère souvent coûteuse et inefficace sans coordination avec les partenaires commerciaux. Dans ce contexte, les organisations régionales apparaissent comme des acteurs stratégiques pour faciliter la mise à niveau normative, à travers des processus d'harmonisation ou de reconnaissance mutuelle.

2.2 Vers une recomposition des alliances stratégiques régionales ?

Un des aspects fondamentaux qui ressort lorsqu'on analyse le manque d'implication des pays en développement dans les processus normatifs est leur isolement. Il apparaît ainsi que les pays les moins développés font face à une véritable barrière dans l'accès à la normalisation, lié à des facteurs divers, qui semble difficile à franchir. Non seulement les facteurs économiques sont un obstacle à l'investissement de ces pays dans les processus normatifs internationaux, mais ce manque d'investissement, en retour, tend à enfermer ces pays dans des espaces normatifs en vase clos, ce qui ne favorise pas les investissements étrangers dans ces espaces qui sont perçus comme une « Terra Incognita » normative. Ce cercle vicieux maintient alors les pays en développement en dehors de l'espace normatif international et constitue un véritable obstacle à leur industrialisation et à leur développement. De plus, la mondialisation du commerce a entraîné une augmentation significative des importations dans les économies en développement, exposant les marchés intérieurs à des produits de qualité inégale, parfois non conformes aux exigences de sécurité ou environnementales. Parallèlement, l'accès aux marchés extérieurs est de plus en plus conditionné au respect de normes techniques rigoureuses, généralement élaborées par les pays industrialisés. Par exemple, dans les cas où les autorités d'un pays importateur ne reconnaissent pas les résultats des tests de conformité à un standard réalisés dans le pays d'origine, ou lorsque ce dernier ne dispose pas des infrastructures techniques nécessaires pour effectuer les essais requis, les entreprises exportatrices doivent supporter le coût des contrôles supplémentaires imposés par le marché de destination. Par exemple, en Moldavie, les producteurs de noix biologiques destinées à l'exportation vers l'Allemagne doivent, par exemple, renouveler leur certification tous les six mois. Chaque inspection effectuée par un organisme de certification international entraîne des frais substantiels, à hauteur de 5 000 dollars, auxquels s'ajoutent 2 000 dollars pour chaque test de conformité, réalisé à deux étapes clés de la chaîne de production, avant et après transformation. Ces dépenses peuvent atteindre jusqu'à 18 000 dollars par an, une somme considérable pour les entreprises opérant dans une économie émergente comme celle de la Moldavie, qui s'efforce de maintenir sa compétitivité sur les marchés internationaux [999]. Au contraire, la mise en place de standards stricts de la part de l'UE sur ses importations de légumes a renforcé la compétitivité des producteurs de légumes au Sénégal, qui, en s'y pliant, ont pu accroître la désirabilité de leur produit sur les marchés internationaux, entraînant une forte hausse de revenus pour les producteurs sénégalais, malgré l'augmentation du coût de production qu'avait entraîné la conformité

[999] The Republic of Moldova Trade Diagnostic Study, World Bank, Report No. 30998-MD, 2004.

aux standards européens [1000]. Cette double contrainte place les pays en développement face à une nécessité impérieuse de moderniser leur système normatif. Cependant, les difficultés sont nombreuses, absence d'infrastructures de certification, fragmentation institutionnelle, faible implication du secteur privé, ou encore coûts élevés d'adaptation aux standards internationaux. Dans ce contexte, les mécanismes de coopération régionale apparaissent comme une solution intermédiaire, permettant de mutualiser les ressources, d'harmoniser les réglementations et de favoriser une intégration graduelle à l'économie mondiale. En Europe, l'Union européenne présente un excellent exemple de mécanisme d'intégration régionale réussi, accompagné de développement spectaculaire en matière de normes, et, de façon plus générale, d'intégration de ses membres à l'économie mondiale. Aujourd'hui, les organisations régionales ont essaimé sur tous les continents, on compte aujourd'hui des centaines d'organisations régionales et sous-régionales partout dans le monde [1001].

Cependant, tous ces organismes présentent des profils très différents, tant en ce qui a trait à leurs objectifs qu'à leur mode de fonctionnement. Comme le rappelait déjà un rapport du ministère des Affaires étrangères publié en 2001, plusieurs conceptions de l'intégration régionale peuvent coexister : *« L'intégration régionale peut être perçue comme des ensembles plurinationaux permettant de dépasser la rivalité belligène des États. Elle peut également viser à faire coïncider les "zones naturelles" ou réseaux d'échanges transnationaux avec des régulations sociopolitiques et un encadrement institutionnel élargi. Elle peut apparaître enfin comme une réponse à la mondialisation en trouvant une solution médiane entre un souverainisme dépassé et un mondialisme lamineur »*[1002]. Ainsi, les objectifs poursuivis par les membres fondateurs d'une organisation régionale peuvent être de diverses natures. De la même manière, les formes d'expression de l'intégration régionale à travers ces organisations peuvent également varier. Ainsi, dans les pays en développement, l'intégration régionale se caractérise par *« une coordination des politiques économiques ou sociales (union économique), par des projets de coopération mis en place par des acteurs (coopération régionale ou fonctionnelle), par des interdépendances entre les économies conduisant à des convergences économiques (intégration des marchés et coopération institutionnelle), par la mise en place de règles ou de transferts de souveraineté munis de structures institutionnelles (intégration institutionnelle ou régionalisme fédérateur), par des relations internationalisées au sein des réseaux ou des firmes (intégration productive ou réticulaire) et par des effets d'agglomération et infrastructures interconnectant au sein des territoires transnationaux »*[1003]. Ainsi, les différents types d'organisations régionales agglomèrent

[1000] Maertens Miet et Swinnen Johan F.M., « Trade, Standards, and Poverty: Evidence from Senegal », *World Development* Vol. 37, No. 1, pp. 161–178, 2009

[1001] https://en.wikipedia.org/wiki/List_of_regional_organizations_by_population

[1002] Hugon Philippe et coll., « Rapport d'analyse comparative des processus d'intégration économique régionale, Paris, Ministère français des affaires étrangères », 2001, p. 8.

[1003] Ibid, p. 7.

des réalités très différentes, allant de simples accords commerciaux sur la réduction des droits de douane, à de véritables organisations transnationales impliquant des transferts de souveraineté et des clauses sécuritaires. Il convient également de noter que les organisations régionales sont le fruit de contextes sociaux historiques divers, qui influent également sur la façon dont les pays membres les perçoivent et interagissent en leur sein. De même, il ne faut pas oublier que de nombreuses organisations régionales doivent se coordonner avec d'autres organisations sous-régionales, dessinant des espaces très diversifiés. Le continent européen fait ici figure d'exception, puisque l'UE constitue la seule organisation régionale d'envergure, sans équivalent sous-régional en Europe.

Au sein des organisations régionales, les accords commerciaux régionaux (ACR) peuvent servir de catalyseur pour le renforcement des capacités normatives. Deux grandes approches se dégagent. Tout d'abord, l'harmonisation directe avec les normes internationales (« en une fois ») et l'harmonisation progressive vers un standard régional intermédiaire. L'ASEAN constitue un exemple emblématique d'approche régionale « en une fois ». Elle a adopté des normes régionales directement alignées sur les standards internationaux dans des secteurs stratégiques, tels que l'électronique. Cette stratégie a permis d'accroître la compétitivité des produits régionaux, tout en facilitant leur accès aux marchés mondiaux [1004]. L'intégration rapide de normes communes a aussi contribué à une meilleure fragmentation de la production entre les pays membres, notamment pour les composants informatiques. Le Mercosur, de son côté, suit une logique d'harmonisation progressive. Il a notamment harmonisé les réglementations techniques relatives aux produits laitiers et aux véhicules, ce qui a permis une forte augmentation du commerce intrarégional dans ces secteurs [1005]. De même, la mise en place de standards sanitaires communs pour les cosmétiques et les colorants alimentaires a réduit les obstacles techniques au commerce. La Communauté andine présente un modèle hybride, où l'harmonisation des réglementations s'accompagne d'une reconnaissance mutuelle des certificats de conformité. L'adoption de la décision 506[1006] a permis aux produits certifiés par des laboratoires accrédités dans un pays membre d'être acceptés dans les autres pays de la région. Cela a réduit les coûts de mise en conformité pour les entreprises exportatrices et amélioré la fluidité du commerce régional.

Ainsi, il apparaît que les avantages des approches régionales sont multiples : réduction des coûts de transaction, création d'économies d'échelle, amélioration de la qualité des produits, et renforcement de la compétitivité à l'exportation. Ces initiatives permettent aussi une meilleure articulation entre normes techniques et procédures d'évaluation de la conformité (tests, certification, accréditation), condition nécessaire à leur reconnaissance mutuelle. Les organisations régionales facilitent la création

[1004] Aldaz-Carroll, E., « Regional Approaches to Better Standards Systems », World Bank Policy Research Working Paper 3948, 2006, p. 9.
[1005] Ibid, p. 17.
[1006] Ibid, p. 24.

de structures partagées : laboratoires, instances d'accréditation, centres d'information. Elles permettent aussi une participation plus structurée à l'élaboration des normes internationales (ex. : ISO, Codex), en constituant des positions communes. Ce travail collectif peut atténuer la sous-représentation chronique des pays du Sud global dans les arènes normatives mondiales. En outre, les interactions régionales favorisent l'émergence d'une « culture de la normalisation », encore peu ancrée dans nombre de pays en développement [1007]. Par des mécanismes de pression par les pairs, d'apprentissage mutuel et de transferts de compétences, les ACR renforcent les capacités institutionnelles et techniques à long terme.

Cependant, malgré leurs avantages, les intégrations régionales ne sont pas exemptes de risques. La complexité des processus de convergence, la disparité des niveaux de développement entre membres, coûts d'ajustement pour les pays les moins avancés, ou encore le désalignement avec les standards mondiaux sont autant de risques à prendre en compte. Il convient donc de veiller à ce que les normes régionales ne créent pas de nouvelles barrières commerciales à l'égard des partenaires extrarégionaux. La mise en place d'institutions régionales fortes, la transparence des processus d'harmonisation, et l'implication effective du secteur privé sont autant de conditions pour assurer la pertinence et la durabilité de ces initiatives. Ainsi, l'étude de Chen et Mattoo (2004) [1008] souligne que les accords régionaux relatifs aux normes peuvent produire des effets ambivalents sur le commerce international. Si l'harmonisation technique favorise l'intégration entre pays membres et les exportateurs avancés, elle peut en revanche pénaliser les pays en développement non membres, en élevant les coûts d'accès au marché. Les ACR, lorsqu'ils incluent des règles sur l'origine des produits trop restrictives, peuvent accentuer cette fragmentation en favorisant les seuls partenaires régionaux. Ainsi, les organisations régionales ne garantissent pas nécessairement une dynamique inclusive. Leur potentiel dépend des modalités d'intégration : les arrangements qui promeuvent une reconnaissance ouverte et des normes adaptées aux capacités locales renforcent les pays en développement, à l'inverse, ceux qui imposent des standards trop exigeants ou discriminants peuvent accroître leur marginalisation [1009]. Cette analyse plaide pour une gouvernance régionale plus équitable, articulée avec des mécanismes multilatéraux destinés à encadrer les effets d'exclusion. Une réforme des règles commerciales internationales, incluant des limites sur les règles d'origine dans les ACR, serait ainsi souhaitable pour garantir une régionalisation inclusive et compatible avec le développement.

[1007] Valery Tayo Tene Christian, Yuriev Alexander et Boiral Olivier, « Adopting ISO Management Standards in Africa: Barriers and Cultural Challenges », in Heras-Saizarbitoria, I. (eds.) ISO 9001, ISO 14001, and New Management Standards., Measuring Operations Performance., Springer, Cham. https://doi.org/10.1007/978-3-319-65675-5

[1008] Chen Maggie Xiaoyang, et Mattoo Aaditya, « Regionalism in Standards: Good or Bad for Trade? », World Bank, octobre 2004.

[1009] Jaffee, S, et Henson, S., « Standards and Agro-Food Exports from Developing Countries: Rebalancing the Debate », World Bank, 2004.

Dans le contexte du développement régional et de l'intégration économique, la question de la normalisation des données géographiques revêt une importance croissante. Les données géographiques sont devenues essentielles à la planification du territoire, à la gestion des infrastructures, à l'agriculture de précision, ainsi qu'au suivi des politiques environnementales. Pour les pays en développement, l'accès à des systèmes de données géographiques fiables et interopérables constitue un facteur déterminant pour leur capacité à planifier efficacement et à s'insérer dans des chaînes de valeur régionales. Dans cette optique, des initiatives telles que celles appuyées par l'UN-GGIM encouragent l'adoption de normes internationales communes en matière de données géographiques. Toutefois, ces standards peuvent s'avérer difficiles à appliquer sans soutien technique ou institutionnel adapté. Les organisations régionales peuvent jouer un rôle crucial pour combler ces lacunes, en promouvant des cadres communs de collecte, de traitement et de partage des données spatiales à l'échelle régionale. Des expériences significatives ont émergé, notamment en Afrique, avec la mise en œuvre de l'African Regional Spatial data Infrastructure (ARSDI), soutenue par la Commission économique pour l'Afrique (CEA)[1010]. De telles initiatives visent à harmoniser les standards de données entre États membres, à favoriser l'interopérabilité des systèmes et à développer des plateformes régionales ouvertes, réduisant ainsi les asymétries d'information. De même, dans la région Asie-Pacifique, des projets de coopération technique dans le cadre de l'UN GGIM-AP a permis aux pays à revenu intermédiaire de bénéficier de l'assistance de partenaires plus avancés pour l'intégration des normes ISO 19100 sur les données géospatiales [1011]. À titre d'exemple, l'UN-GGIM a lancé un projet régional de cadre de référence géodésique pour l'Asie-Pacifique ou Asia Pacific Reference Frame (APREF)[1012]. Ce projet vise à favoriser le partage de données GNSS à l'échelle régionale, à développer et maintenir une source fiable de coordonnées et de vitesses pour les stations géodésiques de la région, à travailler en coopération étroite avec le Service international GNSS (IGS) pour créer et entretenir le réseau permanent de stations de référence APREF, et à augmenter significativement la contribution des stations de la région au Système international de référence terrestre (ITRF). Au-delà de ces objectifs techniques, APREF

[1010] United Nations Economic Commission for Africa (ECA), « Developing a Regional Spatial Data Infrastructure in Africa », 2018 ; United Nations Economic Commission for Africa (ECA), « Guidelines for the implementation of national spatial data infrastructure in African countries », 2018.

[1011] UN-GGIM-AP, « Regional Workshop for Promoting the Asia-Pacific Geospatial Information Platform », 16 octobre 2020.

[1012] L'Asia Pacific Reference Frame (APREF) est un projet géodésique régional créé en 2009 à la suite de la 19ème Conférence cartographique régionale des Nations Unies pour l'Asie et le Pacifique, qui a pour objectif de créer et maintenir un cadre géodésique précis répondant aux besoins croissants des industries, des programmes scientifiques et du grand public utilisant des applications de positionnement dans la région Asie-Pacifique. Face à la fragmentation des réseaux de stations GNSS (Global Navigation Satellite System) dans la région, à l'absence de partage systématique des données entre pays et à la faible densité des infrastructures géodésiques comparativement à l'Europe ou aux Amériques, les États membres ont convenu de développer une infrastructure régionale commune permettant d'offrir un accès cohérent, continuellement raffiné et facilement accessible à un système de référence géodésique moderne. Source : Hu, G. et al. (2019). "Report on the Asia Pacific Reference Frame (APREF) Project", UN-GGIM-AP. ; Geoscience Australia (2024). "Asia-Pacific Reference Frame (APREF)".

ambitionne également d'établir un modèle dense de champ de vitesse en Asie et dans le Pacifique pour des applications scientifiques comme l'étude de la tectonique des plaques et la maintenance à long terme du cadre de référence régional, tout en organisant des symposiums réguliers permettant aux acteurs nationaux et régionaux de partager leurs expériences et leurs développements. Le projet repose sur la mise en œuvre des normes internationales de la série ISO 19100 relatives à l'information géographique, garantissant ainsi l'interopérabilité et la cohérence avec les standards mondiaux. La norme ISO 19111 sur le référencement par coordonnées est appliquée systématiquement pour tous les produits APREF, assurant des transformations cohérentes entre les systèmes de référence nationaux et le système international ITRF. La norme ISO 19127 concernant le registre géodésique est implémentée à travers la maintenance d'un Registre géodésique ISO (ISOGR) à long terme, dont l'organe de contrôle comprend des délégués de l'Association internationale de géodésie et des experts géodésiques internationaux. Enfin, la norme ISO 19161-1 relative au Système de référence terrestre international (ITRS) garantit l'alignement rigoureux de l'ensemble du réseau APREF sur le cadre de référence global, contribuant ainsi à sa densification dans une région qui était historiquement sous-représentée. Ainsi, la normalisation des données géographiques s'inscrit pleinement dans les dynamiques régionales de développement normatif. Elle illustre comment les organisations régionales peuvent catalyser l'appropriation de standards globaux tout en les adaptant aux réalités locales. Cette intermédiation est essentielle pour garantir que la révolution numérique et l'expansion des données spatiales bénéficient aussi aux pays les moins dotés en capacités techniques.

Ainsi, face à l'intensification des échanges internationaux et à la montée en puissance des exigences normatives, les pays en développement sont confrontés à la nécessité de moderniser et de renforcer leurs systèmes de normalisation. Dans cette perspective, les organisations régionales apparaissent non seulement comme des instruments de coordination technique, mais également comme des catalyseurs d'intégration économique, de renforcement des capacités institutionnelles et d'influence collective dans les enceintes internationales. Les approches régionales offrent plusieurs bénéfices. Elles permettent notamment de mutualiser les coûts liés à la mise en conformité, de diffuser des savoirs techniques à l'échelle sous-régionale, d'améliorer la qualité des produits et d'ancrer une culture normative partagée. Comme l'illustrent les expériences de l'ASEAN, du Mercosur et de la Communauté andine, les modèles d'harmonisation directe ou progressive, associés à des mécanismes de reconnaissance mutuelle, peuvent contribuer à une amélioration significative de la performance commerciale régionale. Cependant, ces dynamiques ne sont pas exemptes d'ambiguïtés. Ainsi, l'intégration normative régionale peut également engendrer des effets discriminatoires, notamment pour les pays non membres ou ceux dont les capacités techniques sont limitées. L'alignement sur des standards trop élevés, ou l'adoption de règles d'origine restrictives peuvent creuser les écarts au lieu de

les résorber. Ainsi, la gouvernance régionale doit éviter toute fermeture technico-normative qui serait incompatible avec les principes d'inclusion et d'équité du système commercial international. La réussite des intégrations régionales repose donc sur plusieurs conditions. Tout d'abord, la flexibilité des modalités d'harmonisation, mais également l'accompagnement technique des membres les plus fragiles, la transparence des processus, et l'articulation cohérente avec les cadres multilatéraux. Une régionalisation bien conçue peut non seulement renforcer la compétitivité et la résilience des pays en développement, mais aussi servir de tremplin vers une participation plus active et plus équilibrée à la gouvernance globale des normes. Ainsi, si les organisations régionales ne constituent pas nécessairement une panacée pour tous les problèmes rencontrés par les économies émergentes dans leur participation aux instances de normalisation internationales, elles permettent de mettre en commun les ressources des pays en développement afin d'améliorer leur chance de participation.

2.3 Enjeux de souveraineté numérique dans les standards géographiques

La scène internationale contemporaine est dominée par l'émergence d'acteurs régionaux qui défient la prépondérance des grandes puissances occidentales. La Russie, la Chine, la Turquie, ou encore l'Inde, optent pour des stratégies de diplomatie flexible et de partenariat ciblé, souvent bilatéral, qui contrastent avec la rigidité des alliances multilatérales classiques. Cette dynamique favorise des coopérations opportunistes, adaptées aux circonstances, et limite les engagements à long terme qui caractérisaient les alliances du passé. Parallèlement, les dissensions entre alliés sont devenues plus visibles, tant sur les questions de défense que sur les sujets économiques ou technologiques. L'affaire AUKUS (2021), impliquant l'Australie, le Royaume-Uni et les États-Unis, en constitue une illustration notable, révélant les limites de la confiance mutuelle entre alliés historiques [1013]. Ce type de rupture ou de réalignement stratégique met en évidence les tensions structurelles d'un système d'alliances confronté à une multipolarité croissante. De plus, la montée en puissance de nouvelles technologies, en particulier dans les domaines du cyberespace, de l'intelligence artificielle et de la surveillance spatiale, transforme les modalités de la coopération sécuritaire. La compétition pour le contrôle de ces capacités techniques stratégiques alimente des formes de rivalités qui se traduisent rarement par des affrontements directs, mais souvent par des tensions persistantes au sein même des alliances. Les structures d'alliance, pour survivre, se diversifient. On assiste ainsi à une prolifération de formats coopératifs alternatifs. Les « partenariats stratégiques » se sont multipliés, offrant aux États une voie intermédiaire entre l'engagement institutionnel rigide et la simple coopération ponctuelle. La Chine, à titre d'exemple, a fait des partenariats stratégiques un pilier de sa politique extérieure, en particulier en Afrique, en Amérique latine et en Asie-Pacifique[1014]. De même, la Russie développe des alliances de circonstance, adaptées à ses intérêts immédiats, comme le montrent ses coopérations avec l'Iran ou la Syrie[1015].

Dans ce contexte de transformation rapide des équilibres géopolitiques, la question de la souveraineté numérique occupe une place centrale dans les stratégies nationales et régionales de développement technologique. Elle prend une acuité particulière dans le domaine des standards géographiques, qui conditionnent l'interopérabilité, la sécurité et la gouvernance des données issues de

---

[1013] Commission de la défense nationale et des forces armées, « La préparation à la haute intensité », Rapport d'information n° 5054, Assemblée nationale, 17 février 2022, 187 pages, p. 22.

[1014] Zhang Ketian, « Alliances with Chinese characteristics? The contents and rationale of China's strategic partnerships », in *International Politics*, Vol. 62(2), Palgrave Macmillan, 2 juin 2025. https://link.springer.com/article/10.1057/s41311-025-00701-0.

[1015] Nicole Grajewski, « The Evolution of Russian and Iranian Cooperation in Syria », Center for Strategic & International Studies, novembre 2021. https://www.csis.org/analysis/evolution-russian-and-iranian-cooperation-syria.

sources spatiales, cloud et algorithmiques. Comme démontré précédemment, la souveraineté numérique ne se limite pas au simple contrôle des infrastructures, elle implique également la capacité à définir les normes et protocoles techniques structurant l'accès, l'échange et l'exploitation des données géospatiales. Ainsi, face à la recomposition des anciennes alliances, et l'instabilité politique qui en découle, développer et maintenir une autonomie stratégique en matière d'accès et de diffusion des informations géographiques est essentiel. À cet égard, la mise en place de la constellation IRIS² ("Infrastructure for Resilience, Interconnectivity and Security by Satellite"), annoncée par la Commission européenne en 2022, répond à la nécessité de doter l'Union européenne d'une capacité autonome de connectivité spatiale [1016]. Ce projet vise à concurrencer les initiatives américaines, telles que Starlink (SpaceX) ou Project Kuiper (Amazon), qui offrent des services d'Internet satellitaire à large bande. Outre les avantages en matière de connectivité, IRIS² constitue un instrument clé de maîtrise des données géospatiales sensibles, en garantissant leur traitement au sein de l'espace juridique européen.

Pour maximiser l'efficacité opérationnelle et l'impact stratégique d'un programme de connectivité sécurisée, il est essentiel de privilégier une approche fondée sur l'ouverture technologique. Cela implique notamment la promotion de normes techniques accessibles, l'adoption de solutions reposant sur des logiciels libres et le renforcement de l'interopérabilité entre les différents composants de l'architecture numérique. Une telle orientation favoriserait une meilleure intégration entre cette infrastructure et les autres volets du programme spatial de l'Union, tout en facilitant son articulation avec des services ou applications développées à l'échelle nationale. En outre, cette démarche permettrait de réduire les coûts en évitant la redondance dans la conception de systèmes technologiques similaires, d'accroître la fiabilité globale du dispositif, de stimuler l'innovation par l'ouverture des écosystèmes de développement, et de tirer parti des bénéfices associés à une concurrence élargie dans le secteur. L'enjeu de la normalisation apparaît ici primordial : sans normes communes européennes, les différents systèmes satellitaires peuvent être incompatibles ou opérer dans des silos techniques. C'est pourquoi l'Agence de l'Union européenne pour le programme spatial (EUSPA) travaille à l'harmonisation des interfaces de communication, des protocoles de sécurité et des standards d'interopérabilité entre IRIS², Galileo et le programme d'observation de la Terre européen Copernicus. De plus, du fait de sa portée globale, le programme présente une dimension internationale particulièrement marquée. Les services qu'il propose s'adresseront non seulement aux citoyens et aux institutions de l'Union, mais également aux acteurs publics et privés situés hors de ses frontières, contribuant ainsi à renforcer les relations de coopération entre l'Union européenne, ses États membres

[1016] Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027.

et les partenaires étrangers. Cette ouverture offre une opportunité stratégique de valorisation du programme dans le cadre des initiatives de diplomatie technologique. Là encore, le rôle des normes sera clé dans cette politique diplomatique, en aidant au développement de systèmes satellitaires transfrontaliers fondés sur des normes approuvées et adoptées par l'Union.

Le programme Galileo renforce également cette orientation. Déployé sous l'égide de l'Agence spatiale européenne (ESA), il offre un système de positionnement global indépendant du GPS (américain), de GLONASS (russe) ou de BeiDou (chinois). Cette indépendance repose sur des standards propres à l'UE, comme le Service public réglementé (PRS), qui garantit une transmission sécurisée des signaux pour les usages sensibles. Ainsi, l'adoption de normes techniques européennes dans la navigation satellitaire devient un levier de souveraineté à la fois technologique et politique. La défense n'est pas non plus en reste concernant le développement de programmes spatiaux, lancé en 2010, le programme MUSIS (MUltinational Space-based Imaging System) est une initiative européenne visant à remplacer et mutualiser les systèmes d'acquisition d'image satellitaire européens dédiés à la défense (systèmes optiques français Hélios et Pléiades, systèmes radar allemand et italien SAR-Lupe et Cosmo-SkyMed). Ce programme regroupe aujourd'hui la France, l'Allemagne, l'Italie, la Belgique, l'Espagne et la Grèce. Comparé à son prédécesseur Hélios II, ce nouveau programme (MUSIS) représente un saut qualitatif notable. En effet, il permet d'accéder à des images d'une résolution améliorée, d'identifier des cibles plus petites, et d'augmenter significativement le volume quotidien de données disponibles. L'introduction d'un troisième satellite contribue par ailleurs à une réduction sensible du temps de revisite, améliorant ainsi la réactivité opérationnelle. L'harmonisation des normes utilisées par l'ensemble des composantes machines et humaines du programme MUSIS est une part essentielle de la réussite du programme. Ce volet a été pris en charge par l'Organisation conjointe de coopération en matière d'armement (OCCAR)[1017]. Au sein de l'OCCAR, la France et l'Italie se sont associées pour développer la Couche d'Interface commune (Common Interoperability Layer : CIL) du système multinational d'imagerie spatiale (MUSIS). Ainsi, à la suite de l'achèvement de la phase de définition préliminaire du programme (dite « Phase B ») à la fin de l'année 2015, le contrat MUSIS Stage 2 a été signé le 18 novembre 2019. Cet accord a été conclu entre l'agence d'acquisition conjointe OCCAR-EA, agissant pour le compte des nations partenaires, en l'occurrence la France et l'Italie, et un consortium industriel regroupant Thales Alenia Space (Italie) et Airbus Defence and Space. L'objet principal de ce contrat était le développement et la mise en œuvre d'une interface

[1017] L'Organisation conjointe de Coopération en matière d'Armement (OCCAR) a été initialement créée par un Accord administratif signé par les ministres de la Défense de la France, de l'Allemagne, de l'Italie et du Royaume-Uni le 12 novembre 1996. L'objectif de l'OCCAR est d'accroître la coopération en matière d'armement entre les États membres afin d'améliorer l'efficacité des programmes d'armement et de réduire leurs coûts. Source : https://www.occar.int/about-us/history. Consulté le 19 février 2025.

d'interopérabilité (CIL) visant à assurer la compatibilité opérationnelle entre la Composante spatiale optique (CSO) française et les satellites italiens d'observation radar de seconde génération Cosmo-SkyMed. La couche commune interopérable (CIL) sert de pont entre les segments sol utilisateur des systèmes spatiaux français et italien. La CIL permet aux utilisateurs d'un pays d'exploiter les systèmes satellitaires de l'autre pays et de recevoir, stocker et récupérer des images en toute sécurité, garantissant ainsi l'intégration transparente des deux systèmes spatiaux. Après une première phase de qualification, les utilisateurs finaux ont commencé les essais opérationnels du système en novembre 2024[1018]. Le système est aujourd'hui pleinement opérationnel et géré conjointement par Airbus Defense and Space et Telespazio[1019] pour une durée de 15 ans.

À l'ère de la géopolitique des données, différents modèles de développement de normes coexistent difficilement, tant sur les plans juridiques que stratégique. Comme souligné précédemment, si l'Union européenne mise sur une diplomatie normative articulée autour de principes, tels que la transparence, la protection des données personnelles, l'inclusivité et l'ouverture, ce modèle est loin d'être suivis par tous les grands acteurs de la normalisation internationale. Ainsi, l'américain repose historiquement sur un écosystème fortement structuré par le secteur privé. Les entreprises telles que Google, Amazon, Microsoft, Apple ou Esri jouent un rôle moteur dans l'élaboration des standards techniques, notamment à travers des consortiums internationaux (comme l'OGC ou le W3C) où elles occupent une position dominante. Dans le domaine géospatial, Esri impose de facto son format propriétaire (shapefile, geodatabase) dans de nombreuses administrations à travers le monde, sans être adossé à un standard ISO ou ouvert. De plus, l'extraterritorialité du Cloud Act (2018) offre aux autorités américaines un levier juridique pour accéder aux données hébergées sur des serveurs opérés par des entreprises américaines, y compris en dehors du territoire national. Cela renforce la capacité d'influence des États-Unis sur les flux de données géographiques, tout en alimentant les inquiétudes des autres États en matière de confidentialité et de souveraineté. La République populaire de Chine articule sa stratégie autour d'un modèle étatique centralisé, fondé sur une intégration étroite entre les organismes publics, les entreprises technologiques nationales (Huawei, Baidu, Alibaba, Tencent) et les agences de normalisation (SAC – Standardization Administration of China). En matière de géomatique, la Chine s'appuie sur sa constellation BeiDou comme outil d'indépendance stratégique, en promouvant des standards spécifiques (notamment dans les pays partenaires de l'Initiative Belt and Road).

[1018] OCCAR, « MUSIS Common Interoperable Layer (CIL) Delivered », 17 février 2025 https://www.occar.int/news/musis-common-interoperable-layer-cil-delivered consulté le 19 février 2025.

[1019] Telespazio est une coentreprise franco-italienne de l'industrie spatiale spécialisée dans les services liés à la mise en œuvre des satellites. La société fondée en 1961 est devenue une coentreprise franco-italienne à la suite de la fusion en 2005 d'Alcatel Space avec Alenia, devenu Alcatel Alenia Space, puis Thales Alenia Space. La société est détenue à hauteur de 67% par Finmeccanica et à 33% par Thales. Source : https://fr.wikipedia.org/wiki/Telespazio. Consulté le 19 février 2025.

Contrairement au modèle européen, fondé sur la compatibilité et l'interopérabilité ouverte, la Chine développe des standards dits « souverains », souvent non alignés avec les normes ISO/OGC, et dont l'accessibilité est restreinte. Cela favorise une autonomie technologique complète, mais complique les coopérations interopérables avec les systèmes occidentaux. À cet égard, la stratégie « China Standards 2035 » vise explicitement à faire de la Chine un acteur prescripteur de normes internationales, y compris dans les domaines du cloud et de l'intelligence artificielle appliquée à la géographie. Ces divergences ne sont pas seulement techniques, mais traduisent des visions concurrentes du rôle de la norme dans l'économie numérique. Toutefois, certains espaces de convergence émergent, en parallèle à des zones de frictions persistantes.

Malgré leurs antagonismes apparents, les États-Unis, la Chine et l'Union européenne partagent un intérêt commun pour la stabilité des échanges numériques, la fluidité du commerce international et la compatibilité des systèmes critiques. Cette logique favorise l'émergence de « convergences fonctionnelles » dans les enceintes de normalisation multilatérales, comme l'ISO, l'OGC ou l'ITU. Par exemple, la participation de Huawei et de Microsoft aux travaux de l'OGC sur les services géospatiaux cloud native démontre une volonté partagée de répondre à des besoins techniques communs (performance, sécurité, accessibilité) au-delà des clivages géopolitiques. De même, les efforts de corégulation engagés dans les discussions sur les standards de l'IA à l'ISO/IEC JTC 1/SC 42 montrent que la coopération est possible sur des bases techniques [1020]. La reconnaissance mutuelle de certains standards dans les accords commerciaux, comme ceux du CPTPP[1021], suggère également un espace de compromis sur les standards non sensibles, en particulier dans les secteurs civils.

À l'inverse, des lignes de fracture majeures apparaissent sur les sujets touchant à la souveraineté, à la sécurité nationale et à la gouvernance des données. Les mesures extraterritoriales américaines (CLOUD Act, FISA) sont perçues comme un obstacle à l'autonomie numérique des autres acteurs. L'Union européenne, via le RGPD et ses initiatives cloud souverains, tente de réagir par une régulation défensive. La Chine, quant à elle, oppose à cette dynamique une vision souveraine et centralisée, notamment à travers son triple arsenal législatif déployé entre 2017 et 2021 : la Loi sur la Cybersécurité (juin 2017), la Loi sur la Sécurité des Données (septembre 2021) et la Loi sur la Protection des Informations Personnelles (novembre 2021)[1022]. Ces trois lois forment un système intégré plaçant sous contrôle centralisé de l'Administration du Cyberespace de Chine (CAC) l'ensemble des flux de données, avec deux mécanismes particulièrement contraignants. D'une part, l'obligation de

[1020] Groupe de travail ISO/IEC JTC 1/SC 42 Intelligences artificielles. https://www.iso.org/fr/committee/6794475.html

[1021] Le Partenariat transpacifique global et progressiste (PTPGP) désigne un traité de libre-échange entre onze pays de la région de l'Asie-Pacifique. La langue anglaise utilise le nom de Comprehensive and progressive Agreement for Trans-Pacific Partnership (CPTPP). Source : https://www.eurofiscalis.com/lexiques/cptpp/

[1022] Monolith Law Office, Tokyo (2023). "Qu'est-ce que la loi chinoise sur la sécurité des données ? Explication des mesures à prendre pour les entreprises japonaises".

localisation physique en Chine de toute information personnelle ou « importante » collectée sur le territoire chinois, affectant notamment les 1,3 milliard d'appareils connectés déployés dans le pays[1023]. D'autre part, des restrictions drastiques aux transferts transfrontaliers exigeants, pour tout export de données concernant plus d'un million de personnes ou qualifiées d'« importantes », une évaluation de sécurité obligatoire par la CAC, assortie de sanctions pouvant atteindre 1 million de RMB d'amende, deux ans de prison, et l'inscription au système de crédit social national avec interdiction d'exercer pendant trois ans[1024]. Ces dispositifs, dont les définitions délibérément floues (« données importantes », « nécessité stricte ») laissent une large marge discrétionnaire aux autorités, traduisent une conception de la souveraineté numérique nationale radicalement opposée au modèle occidental. Les données collectées en Chine relèvent de facto de la juridiction exclusive de l'État chinois, qui peut examiner et interrompre tout transfert sur un large spectre de raisons[1025]. Ce modèle centralisé se distingue fondamentalement du RGPD européen non seulement par l'absence de la notion d'« intérêt légitime » comme base juridique de traitement, mais surtout par sa finalité première, qui est de protéger la sécurité nationale dans le cyberespace plutôt que les droits individuels[1026]. Ces antagonismes produisent une fragmentation croissante du cyberespace, illustrée par la multiplication des normes non compatibles (ex. formats de géolocalisation propriétaires, Apis fermées, algorithmes d'IA non documentés). Les initiatives chinoises dans les pays partenaires des Nouvelles Routes de la Soie (via BeiDou et des systèmes de géodonnées propriétaires) visent aussi à exporter un modèle normatif alternatif à celui des pays occidentaux. L'UE, cherchant à éviter une dépendance excessive, développe une diplomatie normative visant à imposer ses standards comme norme internationale de référence. Toutefois, cette ambition se heurte à la puissance d'influence économique et industrielle de ses concurrents, particulièrement dans les technologies émergentes. La question de la normalisation géographique devient ainsi un révélateur des tensions systémiques entre globalisation technique et re-territorialisation politique. Elle appelle à une stratégie active de présence dans les enceintes normatives, mais aussi à la constitution de coalitions transnationales autour de principes communs (éthique de l'IA, transparence des données, standards ouverts). Face à ces tensions et aux opportunités précédemment identifiées, l'Union européenne doit se doter d'une stratégie robuste, cohérente et proactive pour affirmer sa souveraineté numérique dans le champ des standards géographiques.

Tout d'abord, l'UE doit accroître sa capacité à initier et coordonner la production de normes techniques dans les enceintes internationales, telles que l'ISO, l'OGC, l'ITU et l'IEC. Cela suppose un

---

[1023] Ibid. La DSL réglemente également les données non électroniques (Article 3).

[1024] Délégués commerciaux Canada (2024). "La loi sur la cybersécurité – Chine". Liste des agences impliquées dans la mise en œuvre.

[1025] Le Monde du Droit (28 septembre 2017). "Loi de Cybersécurité en Chine", p. 1.

[1026] Développez.com (2017). "La nouvelle loi chinoise sur la cybersécurité entre en vigueur le 1er juin".

soutien renforcé aux experts européens siégeant dans les comités techniques, notamment via un financement public ciblé et des dispositifs de formation spécifiques. Un guichet unique pour la normalisation numérique souveraine, à l'instar d'une « Agence européenne des normes stratégiques », pourrait fédérer les initiatives existantes et aligner les efforts des États membres. Par ailleurs, il est nécessaire de mieux articuler les priorités de la recherche européenne (Horizon Europe, Digital Europe Programme) avec les feuilles de route normatives dans les domaines critiques, tels que le cloud souverain, l'IA géospatiale et la géolocalisation satellitaire. L'UE doit intensifier son action diplomatique pour promouvoir ses standards dans les forums régionaux (UA, ASEAN) et au sein des accords bilatéraux ou plurilatéraux de libre-échange. L'insertion systématique de clauses relatives aux standards ouverts, à l'interopérabilité et à la protection des données géographiques devrait devenir un objectif stratégique. Une coordination interinstitutionnelle renforcée (entre la Commission, le SEAE, le Parlement européen et les agences techniques, comme l'EUSPA ou l'ENISA) est indispensable pour donner à cette diplomatie normative une cohérence d'ensemble et une capacité de réaction rapide face aux initiatives concurrentes.

L'Europe doit également accélérer le déploiement de solutions techniques compatibles avec ses standards. Ce soutien passe par des investissements massifs, des achats publics stratégiques, et des critères de conformité standardisée intégrés aux marchés publics. De plus, l'enjeu de souveraineté numérique ne peut être atteint sans une appropriation large des standards ouverts et européens par les administrations, les collectivités territoriales, les industriels et les acteurs de la recherche. L'Union doit encourager l'adoption de formats interopérables (OGC, INSPIRE, ISO 191 xx) dans la gestion des données géographiques, et intégrer ces exigences dans les politiques de transformation numérique et de données ouvertes. Un effort particulier doit viser les PME et les collectivités locales, via des plateformes de formation, des centres de compétences, et des financements incitatifs. L'Union européenne doit également anticiper les futurs enjeux normatifs, tels que la standardisation des interfaces entre IA et données géographiques, protocoles de cybersécurité géospatiale, métadonnées pour données générées automatiquement. Cette prospective normative doit s'appuyer sur des observatoires multidisciplinaires associant chercheurs, industriels, régulateurs et acteurs de la société civile. En somme, seule une approche intégrée combinant normes, infrastructures, diplomatie et culture technique permettra à l'Union européenne de faire de la souveraineté numérique un levier d'autonomie stratégique, d'innovation durable et de compétitivité internationale dans le domaine géospatial.

En conclusion, l'analyse approfondie des enjeux de souveraineté numérique appliqués aux standards géographiques met en évidence un paysage géopolitique en mutation, dans lequel les normes techniques deviennent des instruments centraux de pouvoir. Que ce soit à travers le développement de constellations satellitaires souveraines, la maîtrise des infrastructures cloud ou l'encadrement des

technologies d'intelligence artificielle, la capacité à définir et imposer des standards structure la compétitivité des nations autant que leur autonomie stratégique. Dans ce contexte, l'Union européenne se distingue par une approche normative fondée sur la transparence, l'éthique et la coopération multilatérale. Toutefois, cette ambition est mise à l'épreuve par des stratégies concurrentes, les États-Unis misent sur l'hégémonie industrielle et l'imposition de standards de facto, tandis que la Chine développe un modèle de souveraineté technologique fondé sur la standardisation nationale centralisée. L'Europe, pour préserver sa souveraineté numérique et renforcer sa capacité d'influence, doit impérativement consolider son rôle d'acteur prescripteur au sein des enceintes normatives internationales, tout en renforçant ses infrastructures et en diffusant une culture des standards auprès de ses acteurs économiques et institutionnels. Les scénarios futurs oscillent entre convergence technique et fragmentation normative. Dans ce cadre incertain, seule une stratégie européenne intégrée et anticipatrice permettra de transformer les normes géographiques en levier de souveraineté effective. L'enjeu n'est pas uniquement technique : il est profondément politique, car il engage la capacité de l'Europe à affirmer son modèle de gouvernance du numérique face à des puissances technorégulatrices aux ambitions croissantes.

3. L'impact des standards privés sur les normes publiques

Si les États et les institutions internationales conservent un rôle important dans la production des standards géographiques (via l'ISO, l'OGC ou INSPIRE), la montée en puissance des entreprises privées dans ce champ a profondément modifié l'équilibre normatif. Des géants technologiques comme Google, Microsoft, Amazon, Esri, mais aussi des industriels stratégiques, comme Thales ou Airbus, s'imposent désormais comme producteurs de standards de facto, modifiant les règles du jeu en matière de traitement, de diffusion et d'interopérabilité des données géospatiales. La montée en puissance des standards privés, portés par de grands groupes technologiques et industriels, transforme profondément le paysage de la normalisation dans le domaine des données géographiques. À travers la définition et la diffusion de formats, protocoles ou plateformes propriétaires, des entreprises comme Google, Amazon, Microsoft, Esri, Thales ou Airbus s'imposent comme des faiseurs de normes de facto. Cette dynamique questionne la capacité des États et des instances publiques de normalisation à encadrer la structuration des flux géographiques selon des critères d'intérêt général, de souveraineté et d'interopérabilité ouverte.

3.1. Influence des grands acteurs technologiques

Les géants du numérique GAFAM en tête, exercent une influence considérable dans le domaine de la géomatique, en structurant l'accès, l'usage et le traitement des données spatiales à travers leurs plateformes. Google, par exemple, avec Google Maps, Google Earth Engine et ses API de géolocalisation, domine le marché de la cartographie numérique, imposant ses formats et interfaces propriétaires. Microsoft, via son service Azure Maps[1027], façonne aussi des environnements de traitement géospatial étroitement intégrés à son architecture cloud. Ces entreprises s'impliquent activement dans les organismes de normalisation, tels que l'OGC (Open Geospatial Consortium), ISO/TC 211 ou IEEE Standards Association, mais y interviennent avec des moyens financiers et techniques sans commune mesure avec ceux des acteurs publics ou des ONG. Ce déséquilibre permet une influence structurelle sur la direction prise par certaines normes, notamment dans les domaines de l'interopérabilité des services Web cartographiques (WMS, WFS), des API RESTful ou encore du géocodage basé sur les modèles d'IA propriétaires.

[1027] Azure Maps est une suite de services de géolocalisation basés sur le cloud et fournis par Microsoft dans le cadre de la plateforme azure de l'entreprise. La plateforme fournit des services géospatiaux et de localisation via des API REST et des kits de développement logiciel (SDK). Le service est généralement utilisé pour intégrer des cartes ou des données géospatiales dans des applications. Source : https://en.wikipedia.org/wiki/Azure_Maps.

L'un des cas les plus emblématiques de standard privé dominant dans la géomatique est le shapefile, créé par Esri dans les années 1990. Bien que dépassé techniquement (limites sur la taille des fichiers, absence de support pour les caractères Unicode, topologie simplifiée), il reste largement utilisé en raison de l'hégémonie des logiciels Esri dans les administrations publiques et les institutions de recherche. Cela illustre un verrouillage technologique : les utilisateurs s'alignent sur des standards pour garantir la compatibilité avec les écosystèmes dominants. À cela s'ajoutent l'essor de formats comme KMZ (Google Earth), ou les dépendances aux API de géolocalisation et de routage fournies par Google, intégrées par défaut dans de nombreuses applications publiques ou commerciales. Ce phénomène se traduit par une marginalisation des standards ouverts soutenus par l'OGC, comme GeoPackage, GML, ou WFS 3.0, et les initiatives européennes comme INSPIRE. Ainsi, dans le domaine de la défense, la France, qui cherche à rompre au maximum sa dépendance envers la société ESRI, pousse régulièrement auprès de ses partenaires à l'adoption du format GeoPackage, en particulier dans le cadre des programmes de coproduction militaire auxquels elle participe. Si les avantages du format GeoPackage sont compris par la plupart des experts, le passage du format Shapefile au format GeoPackage ne se fait pas sans heurt. Tout d'abord, la transition vers un nouveau format perturbe les procédures de nombreuses nations participant au programme, car elles ne sont pas disposées à modifier leur cycle de production. La peur de voir les coûts et le temps de production des données augmenter durant la phase de transition constitue un important repoussoir. Le partenariat stratégique avec le DGIWG, en charge de développer des formats conformes aux attentes des pays membres des programmes de coproduction, est ici de toute première importance, car seul un standard estampillé DGIWG pourra se voir accepter par les nations membres du programme. L'implication de la France au sein du panel n° 5 en charge du développement de ce standard est ici capitale pour voir aboutir ses efforts pour l'adoption de ce standard, et rompre avec la dépendance à ESRI. Il faut également souligner que ESRI est régulièrement convié aux réunions des programmes de coproduction afin de présenter les dernières évolutions de ses logiciels et formats de données, qu'ils développent aussi en tenant compte des remarques des nations membres. L'ubiquité de la société ESRI et sa participation active au sein des instances de normalisation en font un acteur incontournable de la production de données géographiques aujourd'hui, mais le risque de dépendance est fort. Le développement de normes ouvertes à l'OGC et l'investissement dans cette démarche visent à réduire les risques de monopole des acteurs tels qu'ESRI. Le verrouillage est aussi économique. Ainsi, les coûts de transition vers des alternatives libres sont souvent élevés (reformation du personnel, migration des données, adaptation des outils), ce qui limite la diffusion des standards publics même lorsqu'ils sont techniquement supérieurs ou juridiquement recommandés.

Dans le domaine des systèmes spatiaux et des services satellitaires, les industriels européens comme Airbus Defence and Space ou Thales Alenia Space sont des acteurs stratégiques majeurs dans la définition des formats et protocoles de traitement des données issues des satellites. Ces entreprises interviennent dans les projets Copernicus, Galileo et IRIS, où elles contribuent à la rédaction de spécifications techniques (formats de télémesure, standards de métadonnées, modèles d'interopérabilité des plateformes). Ces standards sont souvent définis via des structures mixtes associant agences publiques (ESA, EUSPA)[1028], consortiums industriels et groupes de travail normatifs européens (ETSI, CEN/CENELEC). Bien que cette approche vise une autonomie stratégique face aux modèles dominants extraeuropéens (notamment le GPS et les normes américaines MIL-STD)[1029], elle soulève des tensions sur l'équilibre entre souveraineté publique et intérêts industriels. Certaines spécifications produites restent non publiées ou difficiles d'accès, ce qui limite leur réutilisation par de tiers non-partenaires.

Ainsi, la mainmise des standards privés dans la chaîne de valeur des données géographiques engendre des effets importants sur la capacité des acteurs publics à réguler, exploiter et pérenniser leurs données. Au niveau européen, des initiatives existent pour inverser cette tendance, comme le renforcement du cadre juridique (Data Act, AI Act), la promotion des formats INSPIRE dans les directives nationales, la création d'infrastructures ouvertes, comme GeoNetwork, GeoServer, et le financement de projets de transition vers des logiciels libres dans les SIG publics, via le programme CEF Digital ou Horizon Europe[1030]. Si l'importance de l'autonomie technologique de l'Europe semble donc bien prise en compte au niveau politique, la réalité économique du quasi-monopole de certains acteurs privés au sein de l'écosystème géospatial fait toujours peser un risque sur cette autonomie à long terme, en particulier dans le cadre de l'augmentation des tensions géopolitiques actuelles.

De fait, il apparaît aujourd'hui que les standards privés occupent désormais une place centrale dans l'organisation du secteur géospatial. Formats propriétaires, API fermées, et participation asymétrique aux comités de normalisation sont autant d'éléments qui limitent l'autonomie des institutions publiques à structurer la gouvernance des données territoriales selon leurs propres priorités. Cette situation comporte des risques importants, à commencer par une perte de souveraineté, la fragmentation des systèmes d'information, une dépendance technique accrue, et des difficulté à garantir des principes de transparence, d'interopérabilité et de durabilité dans la gestion des données. Cela nécessite une réponse politique concertée, qui mette l'accent sur le renforcement des compétences gouvernementales en matière de standardisation, sur un appui concret pour les logiciels open source et

---

[1028] L'Agence Spatiale européenne et l'Agence de l'Union européenne pour le programme spatial.

[1029] L'acronyme MIL STD désigne les normes militaires employées par le Département de la Défense américain.

[1030] Commission européenne, « Journée d'information MIE numérique », 11 décembre 2024. https://www.entreprises.gouv.fr/files/files/Evenements/2024/Info%20Day%20-%20CEF%20Digital_PPT%20Presentation_French_Final%20-%2011122024%20%28002%29.pdf. Consulté 30 mars 2025.

les normes ouvertes, ainsi que sur une surveillance accrue des pratiques d'approvisionnement numérique. Dans un contexte de numérisation accélérée des politiques publiques territoriales et environnementales, la reconquête de la maîtrise normative en géomatique ne relève pas seulement d'un enjeu technique, elle est au cœur d'un projet politique de souveraineté numérique européenne. Ce déplacement du pouvoir normatif menace à la fois l'interopérabilité, la transparence et la souveraineté des politiques de données territoriales.

3.2. La bataille autour des formats ouverts vs propriétaires

Dans un contexte où les données géographiques constituent un actif stratégique essentiel à la gouvernance publique, à la planification territoriale et à la sécurité, la manière dont ces données sont structurées, stockées et diffusées est devenue un enjeu politique majeur. Or, ce sont les formats dans lesquels ces données sont encodées qui en déterminent l'accessibilité, la réutilisabilité et l'interopérabilité. Dès lors, le choix entre formats ouverts et formats propriétaires ne relève pas d'une simple préférence technique, il reflète des rapports de pouvoir, des logiques économiques et des visions divergentes de l'intérêt général. Cette sous-partie propose une analyse détaillée des implications de cette opposition, en lien avec la souveraineté numérique des institutions publiques, et notamment de l'Union européenne. Ainsi, la structuration des données géographiques repose sur des formats qui déterminent leur capacité à être partagées, réutilisées, stockées et traitées. Au fil des décennies, une ligne de fracture s'est dessinée entre deux grands paradigmes : d'un côté, les formats ouverts, conçus pour assurer transparence, interopérabilité et pérennité et de l'autre, les formats propriétaires, généralement développés par des entreprises privées et qui tendent à enfermer les utilisateurs dans des écosystèmes techniques spécifiques.

Les formats ouverts désignent des spécifications publiquement disponibles, maintenues par des organismes de normalisation, telles que l'OGC, l'ISO ou encore le programme INSPIRE de la Commission européenne. Leur principal objectif est d'assurer l'accessibilité des données à l'ensemble des acteurs, indépendamment de leur environnement logiciel ou matériel. Parmi les plus répandus dans le domaine géospatial, on retrouve GeoJSON[1031], un format léger utilisé notamment pour l'échange de données vecteurs via des applications Web, le Geography Markup Language (GML), standardisé par

[1031] GeoJSON est un format d'échange de données géospatiales créé par l'IETF, basé sur la notation d'objets JavaScript (JSON). Il définit plusieurs types d'objets JSON et la manière dont ils sont combinés pour représenter des données sur les entités géographiques, leurs propriétés et leurs étendues spatiales. GeoJSON utilise un système de référence de coordonnées géographiques, le Système géodésique mondial 1984, et des unités de degrés décimaux. https://datatracker.ietf.org/doc/html/rfc7946

l'OGC et l'ISO (ISO 19136)[1032], permettant une représentation structurée des objets géographiques. Le GeoPackage, qui repose sur la base de données SQLite pour stocker des données spatiales raster et vecteurs, ainsi que les protocoles d'accès aux services cartographiques WMS et WFS. Ces formats permettent de garantir l'interopérabilité entre les systèmes, d'éviter l'obsolescence logicielle, et d'assurer un contrôle public sur l'architecture des systèmes d'information géographique. Ils sont portés par des institutions comme l'OGC où le programme INSPIRE de la Commission européenne, qui imposent l'usage de formats ouverts dans les infrastructures de données spatiales publiques.

À l'inverse, de nombreux formats sont développés par des entreprises privées dans une logique d'optimisation interne et de domination commerciale. Esri a réussi à imposer le shapefile comme format de référence dans les années 1990, bien que celui-ci présente aujourd'hui de nombreuses limitations techniques[1033]. Plus récemment, Esri a développé le fichier Geodatabase[1034], performant, mais non documenté publiquement dans son intégralité, rendant difficile toute interopérabilité hors de son écosystème logiciel. De son côté, Google a promu le format KML (Keyhole Markup Language) via son outil Google Earth, qui, bien qu'ensuite normalisé par l'OGC[1035], conserve des extensions propriétaires uniquement interprétables par les services Google. Ces formats, souvent optimisés pour un écosystème fermé, créent des effets de dépendance (lock-in) : une fois les données stockées ou traitées dans ces formats, les utilisateurs doivent conserver les outils compatibles, sous peine de perte d'accès ou de qualité. Cela affecte directement les collectivités locales, les agences publiques, et les organismes de recherche, qui doivent parfois investir lourdement pour migrer leurs infrastructures vers des standards ouverts.

Au-delà des considérations techniques, le choix entre formats ouverts et formats propriétaires a un impact profond sur la gouvernance des données. L'adoption de formats fermés entraîne une série de contraintes, à commencer par des coûts récurrents liés aux licences logicielles, à la maintenance et aux mises à jour imposées par les éditeurs. S'y ajoutent des obstacles en matière de transparence, puisque le fonctionnement des formats propriétaires repose souvent sur des spécifications non publiques, limitant ainsi l'auditabilité des systèmes. Enfin, le risque d'indisponibilité ou de retrait d'un produit commercial accroît la vulnérabilité des institutions dépendantes de ces formats. Les formats ouverts, quant à eux, favorisent la mutualisation des ressources entre institutions, garantissent la pérennité des systèmes d'information, et renforcent la capacité de contrôle public sur les données. Ils sont également essentiels

---

[1032] ISO 19136-1 : 2020. Information géographique — Langage de balisage en géographie (GML). https://www.iso.org/fr/standard/75676.html.

[1033] Cepicky Jachym, Switch from Shapefile, 8 octobre 2017 http://switchfromshapefile.org/#nocrs

[1034] Au niveau le plus élémentaire, une géodatabase ArcGIS est une collection d'ensembles de données géographiques de différents types conservés dans un dossier commun du système de fichiers ou dans un système de gestion de base de données relationnelle partagée. Source : https://pro.arcgis.com/en/pro-app/latest/help/data/geodatabases/overview/what-is-a-geodatabase-.htm.

[1035] OGC, OGC KML 2.3, 4 août 2015. https://www.ogc.org/standards/kml/.

au développement de solutions libres, à l'innovation citoyenne, à la recherche scientifique reproductible et à l'accès équitable aux services numériques territoriaux. Ces vertus sont reconnues par la directive INSPIRE, qui impose aux États membres l'usage de formats ouverts pour la diffusion des données spatiales d'intérêt public. La stratégie européenne pour les données, adoptée en 2020, confirme cet engagement en plaçant l'ouverture et la souveraineté au cœur de sa vision de l'économie numérique [1036].

Pour consolider les acquis réglementaires et inverser la dépendance technologique observée dans les services publics, plusieurs orientations stratégiques peuvent être envisagées. La première consiste à insérer, dans les marchés publics numériques, des clauses explicites de préférence pour les formats ouverts. Cela permettrait de conditionner le financement public à la conformité aux standards de l'OGC ou à la compatibilité avec les logiciels libres. En parallèle, un soutien financier accru au développement de solutions open source comme QGIS, PostGIS ou GeoServer renforcerait l'écosystème technologique européen. Par ailleurs, un effort doit être consenti pour financer les opérations de migration des bases de données existantes vers des formats interopérables. Il conviendrait également de renforcer la participation des États membres aux travaux des comités de normalisation européens et internationaux, afin de peser davantage sur les orientations techniques futures. Enfin, des structures comme l'Open Source Observatory (OSOR)[1037] ou les programmes comme Interoperable Europe[1038] doivent devenir des piliers d'une politique européenne ambitieuse en faveur d'un socle commun de données géographiques ouvertes, sécurisées et pérennes.

En définitive, la bataille entre formats ouverts et formats propriétaires dans le domaine des données géographiques n'est pas simplement une affaire de standards techniques, mais elle reflète un affrontement plus large entre logiques de privatisation et logiques d'intérêt général, entre dépendance technologique et autonomie institutionnelle. Le choix des formats structure l'écosystème des données, conditionne l'efficacité des politiques publiques, et reflète la capacité des collectivités à maîtriser les outils de leur propre développement numérique. À l'heure où l'UE affirme sa volonté de réguler les infrastructures critiques, le soutien aux formats ouverts apparaît comme un levier indispensable d'une souveraineté géospatiale durable. Ainsi, la distinction entre formats ouverts et propriétaires dans le

---

[1036] Communication de la Commission au Parlement Européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Une stratégie européenne pour les données », Bruxelles, le 19.2.2020, COM(2020) 66 finals., p. 8. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

[1037] L'Open Source Observatory and Repository (OSOR) est un projet en ligne lancé par la Commission européenne dans le cadre du programme IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens), afin de soutenir la distribution et la réutilisation de logiciels développés par ou pour les administrations du secteur public à travers l'Europe, en connectant les services de l'UE et les États membres.

[1038] Règlement (UE) 2024/903 du Parlement Européen et du Conseil du 13 mars 2024 établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union (règlement pour une Europe interopérable), 2024/903, 22 mars 2024. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32024R0903.

champ des données géographiques engage bien plus que des considérations techniques : elle traduit des modèles antagonistes de gouvernance, d'autonomie et de contrôle. Les formats propriétaires, en facilitant l'enfermement des utilisateurs dans des écosystèmes spécifiques, remettent en cause l'indépendance des systèmes d'information publics. Inversement, les formats ouverts permettent non seulement de garantir une meilleure interopérabilité entre systèmes, mais aussi de renforcer la transparence, la durabilité et l'équité d'accès aux données territoriales. La politique européenne en matière de normalisation et d'ouverture des données reconnaît de plus en plus clairement ces enjeux, mais reste confrontée à des dynamiques de marché puissantes et à des inerties institutionnelles. Afin d'assurer une transition efficace vers un écosystème géospatial plus résilient, inclusif et souverain, il est impératif de combiner engagements réglementaires, accompagnement technique et développement de capacités internes au sein des institutions publiques.

3.3 Normes de facto et domination du marché au sein de l'écosystème normatif des données géospatiales

Dans le champ des données géographiques, la normalisation joue un rôle central dans la structuration des systèmes d'information, la circulation des données et l'interopérabilité des infrastructures numériques. Toutefois, à côté des normes officielles, élaborées par des organismes de normalisation reconnus, tels que l'ISO ou l'OGC, s'imposent également des normes dites « de facto », résultant non pas d'un processus formel de concertation, mais d'un usage massif dicté par les dynamiques industrielles et commerciales. Dans un secteur dominé par des acteurs puissants comme Esri, Google ou Microsoft, ces normes de facto s'inscrivent dans une logique de marché qui tend à court-circuiter les mécanismes institutionnels de régulation normative.

Cette sous-partie explore les ressorts de cette domination non officielle, mais très effective, exercée par certains standards techniques dans l'écosystème géospatial. Il examine comment ces normes de facto émergent, se diffusent et structurent l'action publique, tout en analysant les risques qu'elles font peser sur la souveraineté numérique, la gouvernance des données et la capacité de régulation des États. À travers une approche critique et documentée, il s'agit de montrer en quoi la reconnaissance et la régulation de ces normes de facto représentent un enjeu stratégique majeur pour les politiques numériques européennes. L'écosystème normatif des données géospatiales repose sur une pluralité d'acteurs et sur une diversité de mécanismes d'élaboration de normes, allant des standards formellement adoptés par des organismes de normalisation (ISO, OGC, INSPIRE) aux normes de facto imposées par les dynamiques de marché. Cette sous-partie se propose d'analyser les processus à travers

lesquels certaines technologies, formats ou interfaces acquièrent le statut de norme sans être officiellement normalisés, et les implications géopolitiques, économiques et politiques que cette domination du marché exerce sur les politiques publiques de données géographiques.

Les normes de facto désignent des standards largement adoptés dans un secteur, non pas en raison d'une reconnaissance officielle par un organisme de normalisation, mais du fait de leur usage dominant, de leur efficacité perçue ou de leur intégration dans des produits commerciaux populaires. La diffusion des normes de facto dans l'écosystème géospatial résulte de plusieurs mécanismes. Le premier est d'ordre technique : les entreprises détentrices de plateformes dominantes (Esri, Google, Microsoft) intègrent leurs propres formats ou API comme paramètres par défaut, ce qui pousse les utilisateurs à s'y conformer. Le deuxième facteur est économique : les formations professionnelles, la documentation en ligne, les supports communautaires et les partenariats commerciaux sont souvent alignés sur ces outils dominants, renforçant leur intégration dans les pratiques métier. À cela s'ajoute un facteur institutionnel. Dans de nombreux appels d'offres publics ou projets financés par des bailleurs internationaux, l'exigence implicite de compatibilité avec des solutions dominantes sur le marché tend à marginaliser les outils reposant sur des standards ouverts. Ainsi, le succès des produits ArcGIS dans les projets de coopération au développement a contribué à imposer le shapefile comme format pivot dans l'aide au développement territorial, au détriment de formats plus performants et ouverts, comme GML ou GeoPackage. Cette domination crée un verrouillage technologique : les organisations, une fois engagées dans un écosystème fermé, font face à des coûts de sortie élevés en raison de la complexité des migrations, du besoin de requalification des personnels et du risque de perte de données. De plus, l'institutionnalisation des normes de facto dans le domaine géospatial pose des défis majeurs en termes de souveraineté numérique. En contrôlant les formats de données, les plateformes d'accès et les standards d'échange, les entreprises détentrices de normes de facto influencent la structuration des systèmes d'information des administrations, orientent les politiques publiques de l'information géographique, et restreignent les marges de manœuvre des États dans l'élaboration de leur propre stratégie numérique. Ce phénomène s'accentue avec l'internationalisation des plateformes cloud, sur lesquelles reposent de plus en plus les systèmes SIG des collectivités. Par exemple, des services comme Google Maps Platform, Microsoft Azure Maps ou Amazon Location Service intègrent leurs propres standards et protocoles, qui deviennent incontournables pour de nombreux services publics de mobilité, d'urbanisme ou de gestion de crise. L'imposition de ces normes privées n'est pas sans conséquences, elle introduit une dépendance stratégique à des fournisseurs non européens, expose les données territoriales à des juridictions étrangères, et limite l'intégration des données dans des infrastructures souveraines.

Face à la domination croissante des normes de facto, plusieurs stratégies peuvent être envisagées pour rétablir un équilibre au sein de l'écosystème normatif. La première est d'ordre réglementaire : les institutions européennes, via des instruments comme le data Act ou l'Interoperable Europe Act, peuvent imposer des exigences de compatibilité avec les standards ouverts, voire encadrer l'usage exclusif de certains formats propriétaires dans les marchés publics. La deuxième approche est axée sur la stratégie. Elle consiste à accroître la force des institutions publiques pour qu'elles puissent contribuer activement au processus de standardisation officiel, subventionner le développement des logiciels libres, et favoriser l'interopérabilité dans leurs plans de numérisation territoriale. Cela suppose une formation accrue des administrations aux enjeux normatifs, la constitution de communautés de pratique, et la reconnaissance des standards ouverts comme critères de qualité dans les audits numériques. Enfin, une approche diplomatique est nécessaire à l'échelle internationale pour renforcer la reconnaissance des normes européennes dans les enceintes, comme l'ISO, l'OGC ou l'ITU, et pour promouvoir une gouvernance inclusive et transparente des standards techniques dans les projets internationaux. Ainsi, les normes de facto, en s'imposant par la force du marché plutôt que par la délibération institutionnelle, redéfinissent les équilibres entre innovation technologique et régulation publique. Leur rôle structurant dans les pratiques de la géomatique en fait des instruments de pouvoir subtils, mais puissants, capables d'orienter durablement les choix techniques et stratégiques des acteurs publics. Leur généralisation interroge ainsi les principes fondamentaux de la souveraineté numérique, de l'égalité d'accès aux données et de la gouvernance démocratique des infrastructures numériques. Face à cette réalité, il est urgent de renforcer les capacités des institutions publiques à comprendre, encadrer et, lorsque nécessaire, contester les logiques d'enfermement technologique véhiculées par ces standards dominants. L'articulation entre normes formelles et normes de facto ne doit pas être subie, mais pensée comme un enjeu de politique publique. En réaffirmant les principes d'ouverture, d'interopérabilité et de transparence dans la construction des systèmes d'information géographiques, l'Union européenne peut non seulement garantir son autonomie stratégique, mais aussi proposer un modèle alternatif de normalisation numérique, fondé sur l'intérêt général et la soutenabilité des communs informationnels.

Conclusion du chapitre VII

En conclusion de ce chapitre, il peut être constaté que les mutations contemporaines de l'ordre géopolitique mondial redessinent profondément les rapports de force dans la gouvernance des normes techniques, notamment dans le domaine stratégique des données géospatiales numériques. Dans un contexte marqué par l'intensification des rivalités technologiques, la fragmentation des alliances traditionnelles, et la montée en puissance de nouveaux pôles d'influence (Chine, Inde, pays de l'ASEAN, Union africaine), la France et l'Europe se trouvent confrontées à des défis majeurs pour préserver leur capacité normative et assurer leur souveraineté numérique. Ce chapitre a cherché à mettre en lumière les mécanismes par lesquels les recompositions régionales influencent la dynamique des standards avec, d'un côté, l'émergence d'initiatives concurrentes aux formats européens, et de l'autre, l'activation croissante de logiques de coalition Sud-Sud et de forums alternatifs à la normalisation occidentale classique, tels que l'Organisation de coopération de Shanghai ou l'organisation des Nouvelles Routes de la Soie numérique. Ces évolutions participent à un rééquilibrage des pouvoirs dans les instances internationales de standardisation, dans lesquelles les États européens ne peuvent plus présumer d'un leadership automatique. Face à ces tensions, la capacité de la France et de l'Union européenne à promouvoir leurs propres normes, fondées sur l'ouverture, l'interopérabilité, la transparence et la protection des droits fondamentaux, repose désormais sur une stratégie intégrée. Celle-ci suppose un investissement accru dans les infrastructures critiques, une mobilisation diplomatique renforcée dans les enceintes normatives internationales, et un soutien structurant aux acteurs privés et publics engagés dans la coproduction des standards ouverts. Elle implique également une politique active de partenariats avec les pays du Sud autour d'une normalisation inclusive et équitable, à même de contrer les logiques d'exclusion ou de verrouillage technologique imposées par certains modèles propriétaires. Ainsi, l'avenir normatif de la France et de l'Europe dans l'écosystème des technologies géographiques ne se joue pas seulement sur le terrain technique, mais bien sûr celui des choix géopolitiques, industriels et diplomatiques. Il s'agit de faire de la normalisation un outil stratégique de souveraineté, de projection d'influence et de coopération. Dans cette perspective, les normes constituent bien des instruments de politique internationale, engageant des visions du monde concurrentes, des architectures de gouvernance divergentes, et des modèles sociotechniques en compétition.

Chapitre VIII – Le poids des nouvelles technologies dans la reconfiguration des rapports de pouvoir

Si le Chapitre VII a mis en évidence comment les recompositions géopolitiques contemporaines redessinent les rapports de force dans la gouvernance des normes géospatiales, le présent chapitre s'attache à analyser comment les ruptures technologiques en cours transforment à leur tour les conditions mêmes de cette gouvernance. Alors que les rivalités entre blocs, la fragmentation des alliances multilatérales classiques et l'émergence de nouveaux pôles d'influence reconfigurent le paysage institutionnel de la normalisation, les technologies émergentes, comme l’intelligence artificielle, la blockchain, les jumeaux numériques, et l’informatique quantique, s'imposent quant à elles comme des facteurs structurants majeurs, bouleversant tant les modalités techniques de production et de circulation des données géographiques que les équilibres de pouvoir entre acteurs publics et privés, États et entreprises transnationales. Ce chapitre vise à analyser comment ces technologies émergentes reconfigurent les rapports de pouvoir dans l'écosystème normatif des données géospatiales, en examinant successivement trois champs d'innovation majeurs.

La première section porte sur l'intelligence artificielle et la blockchain comme nouveaux terrains de la normalisation. Elle explore les efforts de standardisation des systèmes d'intelligence géospatiale (formats JSON-LD, ontologies RDF/OWL, extensions GeoSPARQL), les applications civiles et militaires de la GeoAI (de la cartographie automatisée au Geospatial Intelligence ou GEOINT), ainsi que les potentialités et les limites de la blockchain pour la certification de l'authenticité des données géographiques. Elle interroge également les enjeux éthiques et réglementaires soulevés par ces technologies, notamment en matière de biais algorithmiques, de surveillance territoriale et de responsabilité en cas de défaillance des systèmes d'IA.

La deuxième section se concentre sur l'essor des jumeaux numériques et des métavers géographiques, en analysant les défis posés par la normalisation des infrastructures de jumeaux numériques territoriaux, les exigences d'interopérabilité entre représentations virtuelles du territoire et données géospatiales de référence, ainsi que les cybermenaces spécifiques associées aux environnements immersifs comme l’usurpation d'identité, la manipulation de données spatiales, ou encore les attaques sur les infrastructures critiques modélisées dans le jumeau numérique.

Enfin, la troisième section aborde la question de la cybersécurité post-quantique et son impact sur les standards géospatiaux. Cette dernière vise à mettre en lumière les vulnérabilités des infrastructures SIG actuelles face à l'émergence de l'informatique quantique, capable de compromettre les algorithmes de chiffrement asymétrique sur lesquels repose la sécurité des échanges de données géographiques sensibles. Elle présente les premiers efforts de normalisation engagés par le NIST, l'ETSI et l'ISO pour développer des algorithmes cryptographiques résistants aux attaques quantiques, et examine les dynamiques de coopération internationale dans ce domaine, marquées à la fois par des logiques de partage technique et par des stratégies de sécurisation souveraine des infrastructures critiques.

1. L’IA et la blockchain comme nouveaux terrains de la normalisation

L'essor de l'intelligence artificielle géospatiale (GeoAI), c'est-à-dire l'application de l'intelligence artificielle aux données et technologies géospatiales pour automatiser l'analyse et l'interprétation d'informations spatiales, transforme profondément notre capacité à analyser et comprendre le monde. Qu'il s'agisse de cartographier l'étalement urbain, de surveiller des écosystèmes vulnérables ou d'analyser des zones de conflit, les algorithmes d'apprentissage automatique et d'apprentissage profond permettent désormais de traiter à grande échelle des volumes de données géographiques qui auraient été impossibles à exploiter manuellement [1039]. Pour exploiter pleinement ce potentiel, une standardisation rigoureuse des formats et modèles de données s’impose. Autrement dit, il faut structurer l’information géographique selon des normes partagées, afin de garantir l’interopérabilité entre systèmes et la synergie fluide entre données géospatiales et algorithmes d’IA. Parmi ces normes, le format JSON-LD[1040] occupe une place particulière en tant que pont entre le Web de données et les données géographiques, aux côtés d’autres standards consacrés, comme GeoJSON[1041] ou GeoSPARQL[1042]. Afin de mieux comprendre l’étendue de l’impact du développement de l’intelligence artificielle sur les normes géographiques, il est nécessaire d’analyser comment l’IA renforce les domaines de la géographie et de la géomatique, mais également d’examiner ses usages dans la géographie militaire. Enfin, les implications stratégiques, géopolitiques, éthiques et de souveraineté nationale soulevées par la normalisation de ces systèmes d’IA géospatiale doivent également être abordées.

[1039] Arundel Samantha, Li Wenwen, Campbell B. Bryan, « Reimagining standardization and geospatial interoperability in today’s GeoAI culture », Association for Computing Machinery, New York, États-Unis, 20 novembre 2023, p. 83 – 84. Disponible ici : https://dl.acm.org/doi/10.1145/3615886.3627744, consulté le 2 mai 2025. ; Esri, . « Qu'est-ce que GeoAI ? Accélération de la génération de données et résolution de problèmes spatiaux », 2024. https://www.esri.com/fr-fr/capabilities/geoai/overview. Consulté le 2 mai 2025.

[1040] OGC EO Dataset Metadata GeoJSON(-LD) Encoding Standard. Cette norme décrit un encodage GeoJSON et JSON LD pour les métadonnées d'observation de la Terre, pour des ensembles de données. Elle peut être appliquée pour coder des métadonnées fondées sur le profil de métadonnées d'observation de la Terre des observations et mesures (O&M) OGC 10-157r4 ou en tant que codage du modèle conceptuel Unified Metadata Model (UMM-G).

[1041] Cf Note 94.

[1042] OGC GeoSPARQL - A Geographic Query Language for RDF Data. L'activité Web sémantique du W3C définit un ensemble de technologies permettant de créer un « Web de données » où les informations sont facilement partagées et réutilisées entre les applications. Certains éléments clés de cette pile technologique sont le modèle de données RDF (Resource Description Framework), RDFS, le langage d'ontologie Web OWL2, le protocole SPARQL et le langage de requête RDF SPARQL. La norme GeoSPARQL de l'OGC permet de représenter et d'interroger des données géospatiales sur le Web sémantique. GeoSPARQL définit un vocabulaire pour représenter les données géospatiales en RDF. Il définit également des extensions au langage de requête SPARQL pour le traitement des données géospatiales. https://www.ogc.org/standards/geosparql/

1.1. Vers une standardisation des systèmes d'intelligence géospatiale

Le JSON-LD (JavaScript Object Notation for Linked Data) est un format léger conçu pour enrichir des données JSON avec des informations de contexte sémantique [1043]. Concrètement, JSON-LD permet d'encapsuler des données liées (Linked data), dans une structure JSON lisible par les humains, tout en les rendant compréhensibles par des machines à l'échelle du Web. Ce format, standardisé par le W3C, facilite l'interopérabilité des données en attachant à chaque champ un vocabulaire ou une ontologie de référence. À titre d'exemple, on peut représenter un point dans l'espace en JSON-LD en associant ses coordonnées à un identifiant unique (URI) défini par une ontologie géographique. Ainsi, JSON-LD constitue ainsi un socle technique pour le Web sémantique géographique, où les entités géographiques peuvent être reliées à d'autres données ouvertes sur le Web. En tant que format fondé sur JSON, il conserve la simplicité et la popularité de ce dernier, tout en permettant une interconnexion des données à l'échelle de l'Internet tout entier. Dans le domaine géospatial, JSON-LD est souvent utilisé en combinaison avec d'autres normes. Ainsi, le standard GeoJSON, très répandu pour encoder des données géographiques, peut être étendu en GeoJSON-LD. GeoJSON, pour rappel, est un format ouvert permettant de représenter des entités géographiques simples et leurs attributs au format JSON. Il s'agit d'un standard de facto, publié initialement en 2008, puis officialisé par l'IETF en 2016 (RFC 7946), largement adopté pour échanger des données cartographiques sur le Web. Toutefois, GeoJSON à lui seul, ne porte pas de sémantique formelle, c'est ici qu'intervient JSON-LD. L'initiative GeoJSON-LD propose un contexte JSON-LD par défaut pour tout document GeoJSON [1044]. Autrement dit, lorsqu'un processeur JSON-LD lit un fichier « GeoJSON » sans contexte spécifié, il peut appliquer ce contexte standardisé afin d'interpréter correctement les termes géospatiaux. Par exemple, les clés, telles que « Feature » ou « Polygon » sont reliées au vocabulaire RDF approprié, de sorte qu'une Feature GeoJSON soit comprise comme une ressource liée possédant géométrie, propriétés et identifiant unique. Ce mariage de GeoJSON et JSON-LD illustre la complémentarité entre simplicité de la donnée géographique brute et richesse de la donnée liée. L'emploi de JSON-LD permet de conserve la facilité d'échange de GeoJSON tout en dotant les objets géographiques d'une identité exploitable par des graphes de connaissances et des algorithmes d'IA.

De plus, un autre pilier de la standardisation géospatiale à l'ère de l'IA est GeoSPARQL, standard publié par l'OGC en 2012. GeoSPARQL définit une ontologie RDF/OWL pour l'information spatiale, ainsi qu'un ensemble d'extensions SPARQL pour effectuer des opérations géospatiales sur des

[1043] https://json-ld.org/. Consulté le 16 avril 2025.
[1044] Gillies Sean, « GeoJSON-LD », 20 décembre 2021. https://geojson.org/geojson-ld/. Consulté le 12 mars 2025.

données RDF[1045]. En pratique, GeoSPARQL permet de représenter des géométries (points, polygones…) sous forme de triplets RDF et de formuler des requêtes spatiales (par exemple, rechercher toutes les entités situées dans un certain polygone) au sein de bases de connaissances. Il fournit aussi des règles d'inférence pour déduire des relations spatiales, comme par exemple, déduire qu'une entité A est voisine de B si leurs géométries sont contiguës[1046]. Au cours de la dernière décennie, GeoSPARQL est devenu le standard sémantique spatial de référence sur le Web des données, étant largement utilisé pour intégrer des informations géographiques hétérogènes et faciliter le raisonnement automatique. Une version 1.1 du standard a été proposée en 2022 pour étendre ses capacités, signe que la communauté continue de faire évoluer ce langage afin de mieux servir les besoins de la GeoAI contemporaine. En d'autres termes, les formats de données standardisés que sont le JSON-LD, le GeoJSON et le GeoSPARQL permettent tous, à leur propre échelle, de structurer les informations géographiques. JSON-LD apporte le cadre générique des données liées, GeoJSON offre un format d'échange pratique pour les géométries et attributs, et GeoSPARQL inscrit le tout dans le formalisme du Web sémantique avec des capacités de recettages spatiaux avancées. Ensemble, ces standards permettent aux systèmes d'IA de comprendre, d'échanger et d'analyser les informations géospatiales avec cohérence. La standardisation des formats et des ontologies permet de réduire les ambiguïtés, d'éviter la perte d'informations lors d'intégrations de données et assure une base commune sur laquelle bâtir des applications intelligentes. Grâce à elle, une application peut, par exemple, agréger des données provenant de différentes sources (capteurs, bases cartographiques, données ouvertes) et les faire analyser par une IA sans se soucier des différences de structure[1047]. Ainsi, l'IGN exploite cette capacité avec un système automatisé agrégeant imagerie Sentinel-2, données OpenStreetMap, alertes Global Forest Watch et cadastre forestier, sans standardisation, chaque format propriétaire nécessiterait des développements coûteux. JSON-LD et GeoSPARQL permettent la conversion automatique vers une structure commune, exploitable par un agent IA qui classifie l'occupation des sols (85-90% précision) et met à jour la cartographie en heures au lieu de mois[1048]. La standardisation facilite ainsi l'exploitation du plein potentiel de l'IA en géomatique et ce, quels que soient les buts visés.

De fait, une fois les données géographiques correctement structurées et enrichies de sens, l'intelligence artificielle peuvent en tirer parti dans de nombreux domaines civils. L'urbanisme et la planification urbaine, par exemple, bénéficient d'outils d'IA capables d'analyser finement l'occupation

---

[1045] J. Car Nicholas et Homburg Timo, « GeoSPARQL 1.1: Motivations, Details and Applications of the Decadal Update to the Most Important Geospatial LOD Standard », International Journal of Geo-Information, 11(2), p. 117, 7 février 2022. Disponible ici : https://www.mdpi.com/2220-9964/11/2/117#metrics. Consulté le 10 février 2025.

[1046] Ibid.

[1047] Le Monde du Droit, « Loi de Cybersécurité en Chine », 28 septembre 2017.

[1048] Makina Corpus, « IA & cartographie : l'IA pour créer des cartes », 2019. https://makina-corpus.com/sig-cartographie/ia-cartographie-lia-pour-creer-des-cartes-article-1. Consult le 15 mars 2025.

des sols et l'évolution des villes. En intégrant des cartes régulièrement mises à jour et annotées, les modèles prédictifs peuvent projeter l'évolution des zones urbaines et aider à identifier les secteurs nécessitant de nouveaux équipements ou aménagements [1049]. Des modèles d'IA géospatiale sont utilisés pour simuler l'impact de projets d'infrastructure sur l'environnement urbain, permettant aux décideurs d'évaluer différents scénarios d'aménagement. Les simulations de risques naturels illustrent particulièrement cette capacité prédictive. Ainsi, en 2025, pour un projet d'aménagement urbain le long d'une rivière soumise à des crues rapides, l'IA générative a été utilisé pour simuler plus de 500 scénarios d'inondation différents, intégrant des projections climatiques variées (intensités de précipitations variables, durées différentes, impacts du changement climatique avec montée des eaux et événements extrêmes plus fréquents) et des hypothèses de défaillance d'infrastructures spécifiques (rupture de digue, saturation de réseaux d'égouts)[1050]. L'intelligence artificielle peut prédire avec une granularité fine où l'eau va s'accumuler, à quelle vitesse, et quels seront les impacts sur les bâtiments, les routes, les populations et les services essentiels. Elle génère des jumeaux numériques du territoire permettant d'expérimenter virtuellement l'impact de différentes interventions : construction d'une digue de 2 mètres le long de la rivière, transformation d'un parking imperméable en parc perméable pour améliorer l'absorption des eaux de ruissellement, création de zones de rétention d'eau[1051]. L'IA peut également créer des animations vidéo montrant heure par heure la progression de l'inondation dans un bassin versant ou un quartier urbain, illustrant les trajectoires d'écoulement, les zones d'accumulation et l'impact sur les infrastructures critiques. Autant d'outils de visualisations particulièrement utiles pour la formation des équipes de crise, la planification des évacuations et la communication publique. Comme le note une analyse, dans l'urbanisme, les données géographiques intelligemment annotées aident à suivre l'expansion urbaine et optimiser les infrastructures publiques, l'IA pouvant même anticiper les besoins futurs en comparant différents plans d'urbanisation[1052]. Ces projections appuyées par la donnée permettent aux villes de mieux planifier leur développement, en évitant par exemple la saturation des transports ou le manque d'espaces verts.

Le domaine de l'environnement et de la gestion des ressources naturelles est un autre bénéficiaire majeur. L'imagerie satellitaire couplée à des algorithmes de vision par ordinateur permet

---

[1049] Chen Jinliu , Gan Wenquan, Liu Ning et al., « Community Quality Evaluation for Socially Sustainable Regeneration: A Study Using Multi-Sourced Geospatial Data and AI-Based Image Semantic Segmentation », International Journal of Geo-Information, 13(5), p. 167, 2024. Disponible ici : https://www.mdpi.com/2220-9964/13/5/167. Consulté le 13 avril 2025.

[1050] The Reveal Insight Project, « Intelligence Artificielle et Smart Cities : Comment l'IA Transforme nos Villes », 6 octobre 2025. https://www.therevealinsightproject.com/blog/limpact-de-lintelligence-artificielle-sur-les-smart-cities.

[1051] Ibid

[1052] Daniella, « Annotations géospatiales en IA : bonnes pratiques pour des données cartographiques fiables », INNOVATIANIA, 30 janvier 2025. https://www.innovatiana.com/post/geospatial-annotation-for-ai. Consulté le 1er mai 2025.

de surveiller en continu les écosystèmes. Des réseaux de neurones de classification détectent automatiquement la déforestation illégale en comparant des images prises à différentes dates, ou identifient des pollutions de cours d'eau à partir de capteurs in situ. Grâce aux données géospatiales standardisées (imagerie alignée sur des référentiels communs, métadonnées cohérentes, etc.), l'IA peut fournir des analyses précises et en temps réel sur l'état de l'environnement. Ainsi, l'IA peut permettre de détecter la présence de nouvelles constructions ou la dégradation d'un habitat naturel dans des zones protégées quasiment en temps réel [1053]. L'analyse automatisée des images par l'IA accélère ainsi considérablement le travail autrefois manuel des cartographes lors de crises, ce qui se traduit potentiellement par des vies sauvées grâce à une meilleure information des secours.

Cette cartographie automatisée est ainsi l'un des apports les plus visibles de l'IA en géomatique. Les tâches de production cartographique, sont aujourd'hui grandement accélérées par les algorithmes d'apprentissage automatique. En France, par exemple, l'IGN intègre du deep learning pour enrichir ses bases de données d'occupation des sols [1054]. L'IA peut classifier automatiquement la couverture du sol avec une précision relativement élevée. Elle excelle également dans la détection de changements en comparant par exemple deux jeux de données temporels, les modèles repèrent instantanément les nouvelles constructions, la progression d'une crue ou les dégâts d'une tempête. Comme le souligne l'IGN, grâce à l'IA, la mise à jour des cartes peut se faire presque en temps réel, ce qui peut s'avérer vital lors de catastrophes naturelles où il faut connaître l'état du terrain en urgence [1055]. Les bénéfices ne sont pas qu'en termes de rapidité, la qualité de l'information géographique s'améliore également. En combinant la puissance des réseaux de neurones et l'expertise des cartographes, on obtient des cartes plus riches, avec des objets mieux identifiés et une précision accrue, sur lesquelles s'appuient les urbanistes et gestionnaires de territoire. L'IA ouvre ainsi la voie à des analyses prédictives en géographie civile en facilitant la modélisation des évolutions territoriales, elle aide à anticiper les problèmes futurs.

En conclusion, dans les domaines civils, l'intelligence géospatiale soutenue par l'IA apporte rapidité, précision et capacité prédictive. Des tâches autrefois manuelles, comme la photo-interprétation ou la mise à jour de carte sont progressivement automatisées, libérant les experts pour des analyses à plus forte valeur ajoutée. L'IA permet de transformer les données géographiques en véritables connaissances décisionnelles, qu'il s'agisse de mieux comprendre la dynamique d'un quartier ou de surveiller la santé des forêts. Les exemples concrets abondent, qu'il s'agisse de systèmes de transport

[1053] Ibid.

[1054] IGN Institut, « Une carte d'occupation du sol pour faciliter le suivi de l'artificialisation », 27 mars 2025. Disponible ici : https://www.ign.fr/institut/une-carte-doccupation-du-sol-pour-faciliter-le-suivi-de-lartificialisation. Consulté le 25 janvier 2025.

[1055] Ibid.

autonomes utilisant des cartes enrichies par l'IA pour naviguer en sécurité [1056], de l'agriculture de précision où des images satellites annotées informent l'agriculteur sur l'état de ses parcelles en chaque point [1057], ou encore de l'analyse géomarketing où la combinaison de données socio-économiques et géographiques aide à choisir l'emplacement optimal d'un commerce [1058]. Ce grand nombre d'applications témoigne d'un véritable changement de paradigme, puisque les données géographiques peuvent dorénavant bénéficier de la puissance de calcul et du croisement des données rendu possible par l'intelligence artificielle. Ce bond technologique n'est rendu réellement possible que grâce à la convergence de normes de données robustes, qui forment les fondements sur lesquels s'appuient les algorithmes d'IA sophistiqués.

De plus, les avancées de l'IA géospatiale ne se limitent pas aux usages civils. Elles jouent un rôle croissant dans le domaine militaire et le renseignement, notamment dans le domaine du GEOINT. La géographie militaire a toujours été un atout stratégique, qui conditionne, comme souligné précédemment, l'analyse du terrain, la logistique, la surveillance ou la planification des manœuvres. Aujourd'hui, l'IA démultiplie ces capacités, en particulier grâce à la fusion de données géospatiales standardisées (images satellites, relevés lidar, cartes) au sein de systèmes intelligents. En matière de surveillance et de renseignement, l'IA géospatiale est devenue indispensable pour traiter la quantité proprement gigantesque de données captées par les capteurs modernes. Par exemple, l'analyse d'images aériennes ou satellitaires par des réseaux de neurones permet de détecter automatiquement des objets d'intérêt militaire, qu'il s'agisse de véhicules, d'infrastructures, ou de mouvements de troupes. Un partenariat récent entre Thales et l'entreprise LuxCarta illustre cette tendance, soulignant que, pour la cartographie et le renseignement militaire, l'IA est particulièrement utile pour la photo-interprétation, étant capable de détecter, interpréter et numériser automatiquement les bâtiments, routes, obstacles, véhicules, etc.,[1059]. Là où des analystes humains mettaient autrefois des heures à scruter des clichés, un modèle d'IA bien entraîné identifie en quelques secondes des changements ou des menaces potentielles. Cette automatisation permet d'accélérer la production d'informations. Ainsi, les cartes militaires peuvent être mises à jour presque en temps réel. Les analystes peuvent se concentrer sur les

---

[1056] Xu Liu, Guilherme V. Nardari, Fernando Cladera Ojeda et al., « Large-scale Autonomous Flight with Real-time Semantic SLAM under Dense Forest Canopy », IEEE Robotics and Automation Letters, 7(2), avril 2022. Disponible ici : https://arxiv.org/abs/2109.06479? Consulté le 12 février 2022.

[1057] Rutuja Gurav, Het Patel, Zhuocheng Shang, et al., « Can SAM recognize crops? Quantifying the zero-shot performance of a semantic segmentation foundation model on generating crop-type maps using satellite imagery for precision agriculture. », AI for Science Workshop, 4 décembre 2023. Disponible ici : https://arxiv.org/abs/2311.15138? Consulté le 12 février 2025.

[1058] Anasse Boutayeb, Iyad Lahsen-chérif et Ahmed El Khadimi, « A comprehensive GeoAI review: Progress, Challenges and Outlooks », 16 décembre 2024. Disponible ici : https://arxiv.org/abs/2412.11643. Consulté le 12 février 2025.

[1059] THALES, « Thales et LuxCarta s'associent dans le renseignement militaire optimisé par une intelligence artificielle », 23 février 2023. https://www.thalesgroup.com/fr/monde/defense/press_release/thales-et-luxcarta-signent-partenariat-proposer-des-solutions

situations complexes au lieu de s'occuper de tâches répétitives. La France a vu émerger des acteurs à la pointe dans ce domaine, tel que Safran.AI (anciennement Preligens), une entreprise pionnière de l'IA géospatiale de défense rachetée par le groupe Safran en 2024. Ses algorithmes d'apprentissage automatique automatisent le traitement des images satellites pour le compte des analystes du renseignement [1060]. Concrètement, Safran.AI fournit aux armées des systèmes capables de balayer en continu des flux d'images et de signaler instantanément toute anomalie (par exemple, un avion apparaissant soudain sur une base aérienne ou un navire dans un port stratégique). Cette capacité de tri et d'alerte automatique est désormais utilisée par le ministère des Armées et par plusieurs alliés, ce qui atteste de son efficacité opérationnelle. Dans le contexte de la surveillance des frontières ou du théâtre d'opérations, l'IA géospatiale offre ainsi un guet automatisé où les drones, satellites et capteurs terrestres alimentent en permanence une base de données spatiale, que l'IA analyse pour repérer toute activité inhabituelle.

Au-delà de la simple détection, l'IA aide aussi à construire une image opérationnelle commune de la situation tactique. L'OTAN, par exemple, investit dans ces technologies pour améliorer sa connaissance en temps réel du champ de bataille. En 2025, l'Alliance a adopté un système d'IA, fondé sur la plateforme Palantir Maven, destinée à fournir une capacité de combat orientée données commune à tous les alliés [1061]. Ce système intègre un large éventail d'applications IA, des modèles de langage aux algorithmes d'apprentissage automatique, afin d'améliorer la fusion du renseignement, le ciblage, la connaissance du champ de bataille et la planification, tout en accélérant la prise de décision. Le programme américain Project Maven illustre également cette évolution. Lancé en 2017 par le Département de la Défense, Maven a été conçu pour appliquer le machine learning et la fusion de données multisources afin d'identifier des cibles potentielles et d'afficher ces informations aux analystes ou combattants via une interface [1062]. Utilisé sur des théâtres récents, ce programme a démontré qu'il était possible de traiter le flux vidéo continu de drones de surveillance et d'en extraire automatiquement des éléments d'intérêt militaire (véhicules suspects, silhouettes humaines armées, etc.), le tout assez rapidement pour influencer une opération en cours [1063]. Cette philosophie, l'IA comme équipier du militaire, est désormais reprise par de nombreuses armées occidentales. L'OTAN,

---

[1060] Jean-Michel Bezat et Alexandre Piquard, « Preligens-Safran : le mariage d'une start-up d'IA de défense avec un grand groupe industriel », Le Monde, 25 juin 2024. https://www.lemonde.fr/economie/article/2024/06/24/preligens-safran-le-mariage-d-une-start-up-d-ia-de-defense-avec-un-grand-groupe-industriel_6243449_3234.html

[1061] NATO, « NATO acquires AI-enabled Warfighting System », 14 avril 2025 https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system-

[1062] O. Work Robert, « Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven) » US DEPUTY SECRETARY OF DÉFENSE, 26 avril 2017. https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf

[1063] Daniel Caballero-Martin, Daniel Caballero-Martin, Jose Manuel Lopez-Guede et coll., « Artificial Intelligence Applied to Drone Control: A State of the Art », Drones, n° 8(7), p. 296, 3 juillet 2024.https://doi.org/10.3390/drones8070296. Consulté le 4 avril 2025.

en adoptant la solution Palantir, cherche justement à doter ses forces d'un outil commun inspiré de Maven, pour améliorer l'interopérabilité des alliés en matière de GEOINT et de commandement assisté par IA.

D'autres applications militaires de l'IA géospatiale peuvent être soulignées. Ainsi, la simulation et l'entraînement profitent largement de ces avancées : la création de jumeaux numériques de terrains ou de zones de conflit, combinant données géographiques 3D et comportements simulés, permet d'entraîner des commandants à réagir à divers scénarios. L'IA peut simuler des mouvements adverses sur le terrain, offrir des adversaires virtuels crédibles dans des exercices, ou tester des plans dans un environnement virtuel réaliste. Par ailleurs, la logistique militaire s'optimise via l'IA géospatiale. Les armées doivent planifier des acheminements complexes de troupes et de matériel, des algorithmes d'optimisation utilisent les données cartographiques (réseau routier, relief, météo) pour calculer les itinéraires les plus efficaces et adaptatifs, réduisant les temps de trajet et évitant les goulots d'étranglement. Des applications concrètes ont montré que des systèmes d'information géographiques intelligents peuvent recommander les meilleurs axes de progression logistique, y compris en zones dépourvues d'infrastructures, en combinant les données de terrain et les capacités des véhicules [1064]. Enfin, au niveau de la planification stratégique, l'IA appliquée à la géographie permet d'explorer des milliers de configurations de manœuvres ou de dispositions de forces et d'en extraire les plus prometteuses. Par exemple, un système d'IA peut aider un état-major à déterminer où positionner des défenses antiaériennes en fonction du relief et des couloirs aériens, ou à identifier les points critiques d'une ligne de ravitaillement ennemie sur une carte pour maximiser l'effet d'une attaque. Ces usages restent cependant encadrés par le facteur humain, le commandement a toujours le dernier mot, mais ils illustrent comment la géographie militaire se dote d'une forme d'intelligence augmentée par l'IA. La rapidité de calcul de l'IA et la précision des données standardisées est destinée à donner aux décideurs un avantage décisif en leur fournissant une connaissance du terrain plus complète et plus à jour que jamais.

Si la standardisation des systèmes d'IA géospatiale ouvre des perspectives intéressantes, elle soulève également d'importantes questions stratégiques, géopolitiques et éthiques. Tout d'abord, la maîtrise de ces technologies devient elle-même un enjeu de puissance. Les nations et alliances qui dominent la « GeoAI » disposent d'un atout renseignement et militaire potentiellement déterminant. À l'inverse, une dépendance envers des solutions étrangères peut constituer une vulnérabilité. C'est pourquoi on observe un mouvement vers l'IA souveraine dans le domaine géospatial : des États

[1064] Ezra Chipatiso, « Application of GIS and Artificial Intelligence in Military Operations: Prospects and Challenges », Space Science Journal, 1(2), pp. 1-7, 10 juin 2024. https://d1wqtxts1xzle7.cloudfront.net/117488285/application_of_gis_and_artificial_intelligence_in_military_operations_prospects_and_challenges_1_-libre.pdf

investissent pour développer chez eux les compétences et infrastructures d'IA appliquées à la géomatique, afin de ne pas être tributaires de puissances concurrentes [1065]. La France, par exemple, a encouragé l'émergence de champions nationaux comme Safran.AI, et a inauguré en 2022 à Rennes le premier centre dédié à l'IA géospatiale souveraine du pays [1066]. Lorsque Safran.AI a été mis en vente en 2023, il a d'ailleurs été explicitement stipulé que le repreneur devrait être un industriel européen, vu le caractère très sensible de ces technologies. Il s'agit ici de conserver le contrôle national (ou tout du moins européen) sur les outils qui analysent les données géographiques stratégiques, en particulier celles issues de satellites ou de drones militaires.

Les enjeux éthiques sont tout aussi cruciaux. L'emploi de l'IA dans la géomatique, particulièrement à des fins militaires ou de surveillance, suscite des interrogations sur le respect des droits et sur la responsabilité. L'IA géospatiale peut, par exemple, conduire à une surveillance massive des populations via l'analyse automatique d'images satellites ou de flux de caméras urbaines. Même dans les applications civiles, la frontière avec la vie privée peut être floue. Ainsi, des images aériennes haute résolution traitée par IA pourraient révéler des informations sensibles sur les comportements individuels (présence dans tel lieu, etc.). Il est donc impératif de définir des cadres éthiques et juridiques pour encadrer ces usages. Par ailleurs, les biais algorithmiques et les erreurs de l'IA peuvent avoir des conséquences graves lorsqu'ils sont transposés dans le monde géospatial. Un modèle entraîné sur des données incomplètes ou biaisées risque de mal détecter certains objets ou de discriminer des zones. De fait, un algorithme uniquement entraîné sur des villes européennes pourrait avoir du mal à détecter des infrastructures ou dans des environnements différents, et inversement. Dans le contexte militaire, une fausse détection ou une classification erronée pourrait mener à une décision grave de conséquences. L'opacité des systèmes d'IA pose également problème. En effet, si une IA de fusion du renseignement recommande une frappe sur une cible, les décideurs doivent comprendre sur quelles bases cette recommandation a été faite. Or, les modèles de deep learning sont souvent des « boîtes noires » difficilement explicables. Ce manque de transparence peut compromettre la responsabilité et la confiance dans le système [1067]. Des experts soulignent que ces outils, censés assister la décision, pourraient paradoxalement diluer la responsabilité morale en rendant plus floue la chaîne de décision [1068]. C'est pourquoi la notion de contrôle humain demeure centrale, les armées et organisations prônent le maintien d'un contrôle humain significatif sur les systèmes d'IA, considéré comme essentiel

[1065] World Economic Forum, « What is 'sovereign AI' and why is the concept so appealing (and fraught)? », 13 novembre 2024 https://www.weforum.org/stories/2024/11/what-is-sovereign-ai-and-why-is-the-concept-so-appealing-and-fraught

[1066] Joutale Fabien, « Près de Rennes, l'intelligence artificielle de Safran facilite la prise de décisions sur le terrain », Ouest France, 23 mai 2025. https://www.ouest-france.fr/bretagne/ille-et-vilaine/pres-de-rennes-lintelligence-artificielle-de-safran-facilite-la-prise-de-decisions-sur-le-terrain-5c185fd6-37d1-11f0-9fac-ce5100d22487. Consulté le 31 mai 2025.

[1067] Nadibaidze, A., Bode, I., & Zhang, Q., « AI in Military Decision Support Systems: A Review of Developments and Debates », Center for War Studies. Novembre 2024. https://findresearcher.sdu.dk/ws/portalfiles/portal/275893410/AI_DSS_report_WEB.pdf. Consulté le 15 janvier 2025.

pour une utilisation éthique et responsable en opération. En France comme ailleurs, les doctrines émergentes insistent sur le fait que l'IA doit rester un outil d'aide à la décision, et non se substituer au commandement, ce dernier devant toujours être en mesure de reprendre la main et de comprendre les limites de l'analyse automatisée.

Enfin, la standardisation elle-même comporte un enjeu stratégique subtil qui celui de la compatibilité et de la dépendance technologique. Adopter des formats standardisés offre l'avantage de l'interopérabilité, mais nécessite aussi des infrastructures adéquates, à commencer par des plateformes de données capables de gérer ces formats. Les pays qui ne disposent pas de ces infrastructures ou compétences pourraient se retrouver dépendants de fournisseurs externes pour la mise en œuvre des standards. D'où l'importance, dans un souci de souveraineté, de développer des capacités nationales pour implémenter et adapter ces normes à ses besoins propres. À l'inverse, une fragmentation des standards, si chaque acteur développe son propre format fermé, nuirait à la coopération et à l'efficacité globale, mais certains pourraient être tentés de le faire pour protéger leurs données. Il y a donc un délicat équilibre entre ouverture et contrôle à trouver. La communauté géospatiale promeut des standards ouverts précisément pour éviter des silos incompatibles, mais l'ouverture doit aller de pair avec des garanties sur la sécurité et la gouvernance des données partagées.

Ainsi, la standardisation des systèmes d'intelligence géospatiale, illustrée par l'adoption de formats tels que JSON-LD, GeoJSON ou GeoSPARQL, s'inscrit au cœur de la transformation numérique de la géographie et de la géomatique. En fournissant un langage commun pour décrire le monde, ces normes permettent à l'IA d'exploiter pleinement la richesse des données spatiales, que ce soit pour planifier des villes plus durables, préserver l'environnement ou assurer la supériorité informationnelle sur un théâtre d'opérations. Des informations structurées de manière optimale permettent de prendre de meilleures décisions. Cela se vérifie dans les projets civils, comme dans les projets militaires. Cependant, ce mouvement vers l'uniformisation technique ne peut être dissocié des enjeux plus larges qu'il engendre. L'IA géospatiale, parce qu'elle touche à la fois aux territoires, à la sécurité et aux libertés, impose une réflexion continue sur la gouvernance des données, l'éthique de son emploi et la souveraineté numérique. Cette dimension souveraine s'est traduite en France par des initiatives concrètes, comme illustré par la formation du CEDIA (Centre dédié à l'Intelligence

[1068] De Ganay Claude et Gouttefarde Fabien. « Rapport d'information de la Commission de la défense et des forces armées de l'Assemblée nationale sur les systèmes d'armes létaux autonomes », n° 3248, 22 juillet 2020.

Artificielle géospatiale souveraine) [1069], ou l'acquisition de Preligens par Safran, évoqué précédemment [1070]. La création du CEDIA accompagne également le contrat TORNADE (240 millions d'euros sur sept ans) notifié par la Direction Générale de l'Armement (DGA) pour développer des capacités nationales autonomes d'analyse automatisée d'imagerie satellitaire par IA[1071]. Ces investissements massifs soulignent que les questions de souveraineté numérique ne sont plus théoriques. Ces dernières se matérialisent par des infrastructures concrètes, des contrats publics stratégiques et des choix d'investissement qui déterminent dès aujourd'hui les rapports de force géopolitiques et la confiance que l'on peut avoir dans ces nouveaux systèmes.

Parmi les évolutions technologiques prometteuses pour le développement de l'industrie géospatiale, la blockchain occupe également une place de choix. En permettant de renforcer l'authentification des données, la technologie blockchain pourrait constituer à l'avenir un chaînon important dans la protection des données géographiques numériques.

[1069] ActuIA (14 février 2025). « Preligens, pionnier français de l'IA appliquée aux données géospatiales, passe sous le giron du groupe Safran ». L'article précise que Preligens « a ouvert des filiales au Royaume-Uni, aux États-Unis, en Allemagne, en Belgique et à Singapour et, en 2022, créé à Rennes CEDIA, le premier centre dédié à l'IA géospatiale souveraine en France, dont Vincent Cornillet a pris la direction en avril dernier ». https://www.actuia.com/actualite/preligens-pionnier-francais-de-lia-appliquee-aux-donnees-geospatiales-passe-sous-le-giron-du-groupe-safran/.

[1070] Ibid.

[1071] Ibid.

1.2. Blockchain et certification de l'authenticité des données géographiques

La technologie blockchain se présente comme un registre numérique distribué et immuable, permettant de consigner des transactions ou des informations au sein d'un réseau d'ordinateurs interconnectés (les nœuds)[1072]. Chaque nouveau bloc de données n'est ajouté à la chaîne qu'après vérification consensuelle par les nœuds du réseau de l'exactitude des informations qu'il contient. Une fois validées et enregistrées, ces informations sont liées cryptographiquement aux blocs précédents, formant une chaîne chronologique inaltérable. Toute tentative de modification a posteriori serait immédiatement détectable, car elle romprait la cohérence cryptographique de l'ensemble. Ce mécanisme procure à la blockchain une intégrité garantie sans autorité centrale, où le système distribué sert d'arbitre collectif de la confiance. Il s'agit là d'un changement de paradigme par rapport aux schémas classiques, où la confiance repose sur un tiers de confiance unique comme l'État. Désormais, un réseau distribué et transparent peut jouer ce rôle, réduisant le risque qu'une entité unique compromise n'altère la fiabilité du registre [1073].

Appliquée au domaine des données géographiques, cette architecture offre un potentiel inédit pour certifier l'authenticité et la provenance des données. Grâce à la cryptographie, chaque enregistrement de coordonnée, de limite cadastrale ou d'image satellite peut être horodaté et signé de manière infalsifiable. Par exemple, une société française a récemment développé une solution de signature électronique s'appuyant sur la blockchain publique Tezos, assurant l'authentification, l'horodatage et le stockage immuable des preuves de signature, rendue ainsi valable universellement et indéfiniment[1074]. Transposé aux données géographiques, un tel dispositif permettrait de garantir qu'une donnée a bien été enregistrée à une date donnée et n'a subi aucune altération depuis. Cette promesse intéresse tout particulièrement les gestionnaires de données critiques. En rendant techniquement impossible (ou du moins extrêmement difficile) la falsification ex post d'une base cartographique, la blockchain renforce la confiance dans l'intégrité de ces données, sans exiger de faire appel en permanence à un intermédiaire certificateur. La preuve d'intégrité serait alors apportée par le fonctionnement même du réseau et les algorithmes de consensus.

Il convient toutefois de souligner que la blockchain ne résout pas magiquement tous les problèmes de véracité de l'information. Un registre distribué, si sophistiqué soit-il, n'a de valeur que si les données initiales qu'on y inscrit sont fiables, et si les acteurs ou capteurs qui les alimentent sont

---

[1072] Gautami Tripathi, Mohd Abdul Ahad et Gabriella Casalino, « A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges », Decision Analytics Journal, Vol. 9, 23 décembre 2023. https://www.sciencedirect.com/science/article/pii/S2772662223001844

[1073] OGC, « Geospatial Standardization of Distributed Ledger Technologies », OGC Discussion Paper, 6 juillet 2018. https://docs.ogc.org/dp/18-041r1/18-041r1.html

[1074] Site officiel de Tedji. https://www.coexya.eu/notre-offre/tediji-by-coexya/

dignes de confiance [1075]. Il faut ainsi prendre en compte que la qualité de l'oracle (la source qui injecte une donnée du monde réel dans la blockchain) est déterminante. Dans le cas des données géographiques, cela signifie que la précision du capteur GPS, l'authenticité de la mesure topographique ou la véracité d'un document foncier numérisé doivent être établies au préalable. La blockchain certifie l'intégrité après coup, mais ne garantit pas la véracité a priori du contenu. Cette limite implique, en pratique, de combiner la technologie blockchain avec d'autres mécanismes de validation initiale pour obtenir une chaîne de confiance complète du capteur jusqu'à l'usager final.

Ainsi, grâce à ces propriétés techniques, le recours à la blockchain pour certifier l'authenticité de données géographiques a été expérimenté dans divers contextes, tant civils que militaires. Le cas emblématique est celui du registre foncier. Ainsi, à partir de 2016, la Géorgie s'est illustrée comme pionnière en la matière, en partenariat avec la société Bitfury et l'économiste Hernando de Soto [1076]. L'Agence nationale du registre public géorgienne a intégré la blockchain à son système d'enregistrement cadastral afin de sécuriser les transactions immobilières et prévenir la corruption interne. Concrètement, une blockchain privée a été déployée pour horodater toutes les opérations du cadastre, et un ancrage périodique des données hachées a lieu sur la blockchain publique Bitcoin. Ce mécanisme hybride assure que, même en cas de compromission du système interne, une altération illégale des titres de propriété serait détectable via la preuve inscrite sur Bitcoin, bénéficiant ainsi de la robustesse mondiale de cette chaîne publique. Selon Forbes, il s'agit du premier projet gouvernemental officiel reposant sur la blockchain Bitcoin pour un registre foncier. En 2018, déjà 1,5 million de titres fonciers géorgiens avaient ainsi été horodatés via la blockchain [1077], signe d'une volonté politique forte de moderniser et sécuriser le cadastre national. L'expérience géorgienne a inspiré de nombreuses initiatives similaires à travers le monde.

Ainsi, en Suède, l'autorité cadastrale (Lantmäteriet) a conduit un projet pilote dès 2016 afin de dématérialiser et accélérer les transactions immobilières grâce à la blockchain [1078]. Partant du constat que la procédure de vente immobilière prenait plusieurs mois en raison d'échanges de documents papier, le Lantmäteriet a expérimenté une plateforme numérique où toutes les étapes, du compromis de vente jusqu'à l'enregistrement final, seraient gérées par smart contract et signatures électroniques, en

---

[1075] Rapport du 117e Congrès des notaires de France, « Les premières expériences de registre immobilier en blockchain », 31 janvier 2021. https://www.rapport-congresdesnotaires.fr/2021-rapport-du-117e-congres/les-premieres-experiences-de-registre-immobilier-en-blockchain

[1076] Shin Laura, « Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury », Forbes, 21 avril 2016. https://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/

[1077] Ibid.

[1078] Lantmäteriet, « The Land Registry in the blockchain A development project with Lantmäteriet (The Swedish Mapping, cadastre and land registration authority), Telia Company, ChromaWay and Kairos Future », juin 2016. https://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

lien avec une blockchain. Ce projet multipartite a impliqué des acteurs technologiques, comme la startup suédoise ChromaWay, qui a mis à disposition sa blockchain Chromia liée à Ethereum, et des Banque Nationale. En juin 2018, une première transaction immobilière simulée en direct a été réalisée avec succès sur cette infrastructure blockchain, démontrant la faisabilité technique du concept. Bien qu'encourageant, le pilote suédois n'a pas encore conduit à un déploiement en production, notamment parce que le cadre juridique et les habitudes institutionnelles nécessitent des adaptations (la validation finale par l'autorité foncière demeure incontournable). Néanmoins, la Suède a montré que la blockchain pouvait réduire drastiquement les délais et le nombre d'intermédiaires dans un processus cadastral, tout en assurant une traçabilité complète des opérations.

Par ailleurs, dans les pays émergents, où les systèmes fonciers sont parfois déficients, la blockchain a suscité l'espoir de sauter une étape de développement institutionnel. Au Ghana, par exemple, une ONG dénommée Bitland a annoncé en 2016 un ambitieux projet de cadastre sur blockchain [1079]. Le Ghana connaît d'importants problèmes de sécurité foncière, une grande partie des terres échappant au registre public et relevant de droits coutumiers, ce qui engendre conflits et fraudes. Bitland proposait d'enregistrer les titres de propriété et transactions foncières dans une blockchain publique, via l'émission d'un token dédié pour représenter les parcelles. Une ICO (offre initiale de jetons) a même été lancée pour financer l'initiative. Toutefois, faute d'appui officiel et, en dépit du battage médiatique initial, le projet est resté au stade expérimental. Après 2017, l'activité de Bitland a diminué. Les sites Web associés ont disparu ou stagné, et les comptes de réseaux sociaux du projet n'ont pas été mis à jour depuis 2018. Une tentative de relance en 2020 a été signalée (nouveau site Web proposant l'enregistrement gratuit de titres), sans qu'il soit clair si la blockchain est réellement utilisée. Ainsi, ce cas met en évidence qu'une technologie seule ne suffit pas à instaurer une nouvelle gouvernance foncière, sans l'adossement à l'État et un écosystème socio-légal favorable, la blockchain ne peut pas, à elle seule, créer la confiance dans des contextes complexes.

Au-delà du cadastre, d'autres usages civils des registres distribués géographiques émergent. L'expérience géorgienne a ainsi fait école en Amérique latine où la Banque interaméricaine de développement, en partenariat avec ChromaWay, a lancé en 2019 des projets pilotes au Pérou, Paraguay et Bolivie pour explorer l'apport de la blockchain dans la gestion foncière [1080]. L'objectif est d'évaluer si cette technologie peut résoudre des problèmes récurrents en assurant l'intégrité des données cadastrales et en impliquant divers acteurs (notaires, banques, administrations) autour d'un

[1079] Huet Jean-Michel, « Les premiers pas concrets de la blockchain en Afrique », La Tribune Afrique, 9 avril 2018. https://afrique.latribune.fr/think-tank/tribunes/2018-04-09/les-premiers-pas-concrets-de-la-blockchain-en-afrique-774614.html

[1080] IDB, « Distributed Ledger Technology (Blockchain): The Future of Land Titling and Registry », 19 juillet 2019 https://www.iadb.org/en/project/RG-T3356

registre partagé. De même, la ville de Rotterdam aux Pays-Bas a expérimenté dès 2016 l'enregistrement de baux locatifs sur une blockchain, en partenariat avec Deloitte, afin de conférer date certaine et intégrité aux contrats de location immobilière[1081]. L'idée était de prévenir les litiges liés à des baux antidatés ou frauduleux (par exemple en cas de squat), en disposant d'une preuve immuable de chaque contrat. Un acteur privé français, la société Olarchy, s'est d'ailleurs positionné sur ce créneau en proposant depuis 2018 une plateforme de gestion locative entièrement numérisée et sécurisée par blockchain.

Parallèlement, des projets plus expérimentaux cherchent à exploiter la blockchain pour créer de nouvelles formes de données géographiques participatives. Le projet FOAM (basé sur Ethereum) illustre cette tendance. FOAM vise à bâtir une carte du monde décentralisée, où les utilisateurs peuvent ajouter et valider des points d'intérêt ou des emplacements géographiques en échange de jetons numériques [1082]. Il met en œuvre un registre original de « coordonnées crypto-spatiales », stockées sur la blockchain, dont la validation est assurée de façon communautaire et incitative. Dans les faits, les participants sont encouragés par des récompenses en tokens à vérifier sur le terrain la véracité d'une donnée géographique, créant ainsi un filet de sécurité participatif contre les fausses informations. Le protocole FOAM, open source, ambitionne de devenir un standard pour ce type de preuve de localisation décentralisée. Si cela venait à être le cas, un écosystème où des bases de données géographiques concurrentes (ou complémentaires) des bases officielles coexistent, l'une gérée hiérarchiquement par l'État, l'autre émergente et autorégulée par une multitude d'agents, pourrait voir le jour. Cela soulève des questions cruciales sur l'autorité de la donnée géographique.

Le domaine spatial est également concerné par le développement de la blockchain. Ainsi, la NASA étudie l'usage de smart contracts sur Ethereum pour automatiser la coordination de ses capteurs d'observation de la Terre au sein du programme SensorWeb[1083]. Ce programme cherche à créer un environnement interopérable où des satellites et capteurs terrestres déclencheraient des observations de manière réactive en fonction d'événements précis comme un tremblement de terre. La blockchain pourrait servir à enregistrer et propager de façon fiable les réquisitions d'images ou les plans de vol entre satellites, en tirant parti des standards OGC déjà utilisés (Sensor Observation Service, etc.)[1084]. De son côté, l'Agence spatiale européenne s'intéresse aussi aux blockchains dans sa vision Space 4.0, où

[1081] Zadra-Veil, C. (dir.)., « Blockchain & immobilier : le smart bail », Groupe ESPI, octobre 2021. https://hal.science/hal-03419938v1/file/livre-blanc-blockchain-immobilier.pdf

[1082] OGC, « Geospatial Standardization of Distributed Ledger Technologies », OGC Discussion Paper, 6 juillet 2018. https://docs.ogc.org/dp/18041r1/18041r1.html

[1083] Graham Karen, « NASA to use blockchain tech in distributed spacecraft missions », Digital Journal, 1er février 2018. https://www.digitaljournal.com/tech-science/nasa-s-blockchain-tech-will-allow-unmanned-spacecraft-to-think/article/513781#ixzz5CS2pHLg9

[1084] OGC, « SWE Implementation Maturity Engineering Report », 2013.https://portal.opengeospatial.org/files/?artifact_id=53823

une pluralité d'acteurs (privés, universitaires, grand public) participerait aux activités spatiales [1085]. Si ces explorations en sont à un stade préliminaire, elles témoignent du potentiel transversal de la blockchain, jusque dans la gestion des données géophysiques et environnementales globales.

Dans le milieu militaire, où l'information géographique joue historiquement un rôle stratégique, la blockchain suscite également de l'intérêt pour sécuriser les échanges de données sensibles. Le Département de la Défense américain, par exemple, a été encouragé par le Congrès en 2024, à étudier comment la blockchain pourrait renforcer la sécurité des communications opérationnelles [1086]. L'une des pistes envisagées est d'utiliser un registre distribué pour protéger les vastes flux de données échangés entre unités militaires, en particulier en situation de combat. De même, la traçabilité logistique offerte par les chaînes de blocs pourrait permettre de suivre les mouvements de troupes, de carburant ou de matériel tout au long de la chaîne d'approvisionnement, sans risquer qu'un adversaire n'en altère ou n'intercepte discrètement les informations. On voit donc se dessiner l'image d'armées exploitant des ledgers partagés entre alliés pour garantir l'intégrité de leurs données tactiques ou de soutien, là où autrefois seul un chiffrement point-à-point ou des réseaux centralisés sécurisés étaient envisageables. Plusieurs forces armées, dont l'armée française, mènent d'ailleurs des projets pilotes intégrant la blockchain dans des applications non financières : par exemple pour certifier l'intégrité de fichiers de pièces détachées et de plans d'imprimantes 3D destinés à la maintenance sur le terrain [1087]. Dans le projet FIBR2EO de l'armée de Terre, chaque modèle 3D de pièce est enregistré dans une blockchain pour s'assurer que les objets imprimés correspondent exactement au fichier d'origine, avec à la clé une meilleure confiance dans la chaîne logistique des pièces de rechange. Ces exemples, civils comme militaires, convergent vers un constat, qui est que la blockchain apporte une infrastructure de confiance distribuée qui peut, dans des contextes variés, renforcer l'authenticité et la traçabilité des données géolocalisées. Il reste cependant à encadrer son usage et à en maîtriser les implications, ce qui fait l'objet de nombreux débats.

Ainsi, les premières applications de la blockchain géospatiale, aussi prometteuses soient-elles, ont mis en lumière d'importants défis en matière de normalisation. Tout d'abord se pose la question de l'interopérabilité et des standards. En effet, comment intégrer ces nouveaux registres distribués dans l'écosystème existant des données géographiques, qui repose déjà sur des normes établies (formats comme le Geography Markup Language, standards OGC, directives européennes comme INSPIRE,

---

[1085] ESA, « Beyond Bitcoin: Leveraging the Blockchain for Space 4.0 », 6 novembre 2017. https://www.esa.int/About_Us/Digital_Agenda/Beyond_Bitcoin_Leveraging_the_Blockchain_for_Space_4.0

[1086] Base Camp Connect, « Au-delà des cryptomonnaies : Comment la blockchain protège les réseaux gouvernementaux et militaires », 13 novembre 2024.https://basecampconnect.com/fr/blockchain-reseaux-militaires/

[1087] Archives du ministère des Armées, « La blockchain pour appuyer les projets innovants de l'Armée de Terre – le cas de FIBR2EO », 22 juin 2021. https://archives.defense.gouv.fr/terre/pole-numerique-et-innovation/le-numerique/les-projets-numeriques/la-blockchain-pour-appuyer-les-projets-innovants-de-l-armee-de-terre-le-cas-de-fibr2eo.html

etc.) ? De plus, des enjeux juridiques et réglementaires rentrent également en jeu quant à la reconnaissance de la validité de ces enregistrements numériques dans le droit positif (droit de la propriété, protection des données personnelles, etc.). Sur le plan de la standardisation technique, plusieurs initiatives internationales démontrent une mobilisation croissante des instances internationales pour encadrer la convergence entre blockchain et géo-informations. En 2019, l'OGC a créé un groupe de travail dédié aux chaînes de blocs et registres distribués [1088]. L'OGC reconnaît ainsi que ces technologies, initialement popularisées dans la finance (Bitcoin, Ethereum), trouvent désormais des applications dans des domaines tels que le cadastre, les services urbains ou les registres gouvernementaux. L'objectif affiché est double, il s'agit de définir les besoins d'interopérabilité et d'éviter l'enfermement propriétaire en faisant émerger des standards ouverts. Parmi les pistes envisagées figure l'intégration du protocole FOAM évoqué précédemment, ou de son schéma de « coordonnées crypto-spatiales », comme standard OGC à part entière [1089]. En parallèle, au niveau global, l'ISO a mis en place dès 2016 un comité technique spécifique (ISO/TC 307)[1090] consacré aux normes sur la blockchain et les registres distribués. Une trentaine de pays, dont la France, participent à ce comité, qui a déjà produit des référentiels sur la terminologie, l'architecture, la sécurité et la gouvernance des blockchains. S'il ne se focalise pas sur les aspects géospatiaux en particulier, ce cadre ISO a pour but de fournir un socle conceptuel qui facilitera l'adoption cohérente de ces technologies dans divers secteurs, y compris celui de la cartographie et du cadastre. D'autres organisations professionnelles se sont penchées sur ce sujet, à l'instar de la Fédération internationale des Géomètres (FIG), dont les commissions foncières et immobilières étudient les implications de la blockchain pour le métier de géomètre et la gestion cadastrale. Le Groupe de la Banque mondiale a également produit en 2018 des études et guides de bonnes pratiques pour l'usage de la blockchain dans la modernisation des registres fonciers, conscient du potentiel de cette technologie pour améliorer la transparence et l'accès à la propriété dans les pays en développement [1091]. Ainsi, se dessine progressivement un corpus normatif visant à assurer que les solutions de blockchain géospatiale restent interopérables, pérennes et alignées avec les cadres existants de gestion des données.

Du point de vue juridique, plusieurs questions doivent être résolues pour que la blockchain puisse être utilisée à grande échelle dans la certification de données géographiques. La première

---

[1088] OGC, « OGC announces the creation of a new Domain Working Group for Blockchain and Distributed Ledger Technologies », 10 juillet 2019 https://www.ogc.org/announcement/ogc-announces-the-creation-of-a-new-domain-working-group-for-blockchain-and-distributed-ledger-technologies/

[1089] OGC, « Geospatial Standardization of Distributed Ledger Technologies », OGC Discussion Paper, 6 juillet 2018. https://docs.ogc.org/dp/18-041r1/18-041r1.html

[1090] ISO/TC 307 – Blockchain and distributed ledger technologies. https://www.iso.org/committee/6266604.html.

[1091] World Bank Group, « Cryptocurrencies and Blockchain Europe and Central Asia Economic Update », office of the chief Economist, mai 2018. https://openknowledge.worldbank.org/server/api/core/bitstreams/9be74ccf-8280-571a-a3ee-d4daa12fb10a/content

concerne la valeur légale des enregistrements sur blockchain. Dans un système foncier classique, seule l'inscription dans le registre d'État (tenu par une agence gouvernementale ou un notaire public) confère un titre de propriété opposable. Si l'on enregistre une transaction foncière dans une blockchain, comment s'assurer de sa reconnaissance par les tribunaux et les autorités ? L'exemple géorgien a montré qu'une intégration officielle, via un partenariat public-privé, permet d'arriver à une équivalence en droit : en Géorgie, la blockchain est devenue un support technique du registre public, et non un registre parallèle, ce qui évite les conflits juridiques. En Suède, en revanche, le pilote a dû composer avec le droit existant. Les contrats intelligents ne remplacent pas (encore ?) l'acte notarié, ils le complètent dans un environnement de test. De manière générale, l'intégration de la blockchain dans les procédures administratives exige souvent des adaptations législatives ou réglementaires. La France, par exemple, a dû ajuster son droit des sociétés pour reconnaître la transmission de certains titres financiers via blockchain (ordonnance n° 2017-1674 du 8 décembre 2017[1092]), un parallèle qui illustre la nécessité d'une base légale solide. Pour les données géographiques, des réformes similaires pourraient être envisagées. Il faudrait définir quel statut juridique accorder à une preuve d'antériorité ou une signature stockée sur blockchain, et comment articuler ce dispositif avec le rôle des officiers publics.

Un autre défi en matière de normalisation tient au rôle des tiers de confiance et à la gouvernance des chaînes. Paradoxalement, même si la blockchain vise à se passer d'autorité centrale, son déploiement dans le domaine géographique pourrait donner naissance à de nouvelles formes d'intermédiaires ou de régulateurs. Ainsi, la question se pose de savoir qui décide des règles de gestion du réseau dans un contexte étatique. Faut-il une autorité de gouvernance de la blockchain cadastrale, et si oui, comment éviter qu'elle ne redevienne un point de centralisation ou de vulnérabilité ? Plusieurs modèles se dessinent déjà. L'État peut opter pour une blockchain privée ou un consortium, où seules des entités accréditées (ministères, offices notariaux, collectivités locales) opèrent des nœuds validateurs. Ainsi, c'est le choix qu'a fait l'Estonie pour la sécurisation de ses registres. Elle utilise une infrastructure dite de Keyless Signature Infrastructure (KSI, littéralement : infrastructure de signature sans clé), intégrée à son écosystème X-Road d'échange de données administratives [1093]. Cette approche garantit que seules des organisations de confiance contrôlent le registre distribué, tout en bénéficiant de l'horodatage distribué pour détecter la moindre altération de données. D'autres peuvent choisir une blockchain publique, mais hybride, comme la Géorgie l'a fait, pour s'appuyer sur la puissance de calcul mondiale tout en conservant un contrôle sur l'application métier. Chaque choix comporte des

[1092] Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036171908

[1093] Artinovic, I., Kello, L., Sluganovic, I., « Blockchains for Governmental Services: Design Principles, Applications, and Case Studies », Center for technology and Global Affairs, Working Paper Serie n°7, décembre 2017. https://www.ctga.ox.ac.uk/sites/default/files/ctga/documents/media/wp7_martinovickellosluganovic.pdf

implications en matière de normalisation. Une blockchain publique offre plus de résilience et de transparence, mais pose des problèmes de gouvernance. Tandis qu'une blockchain privée donne à l'État la main sur la gouvernance au prix d'une confiance plus restreinte, le modèle centralisé est partiellement conservé, quoiqu'avec des garanties cryptographiques supplémentaires.

L'essor de la blockchain dans le domaine des données géographiques s'inscrit ainsi dans une problématique plus vaste de souveraineté et de reconfiguration des pouvoirs liés à l'information. Historiquement, comme souligné en introduction, la maîtrise de la cartographie et des données territoriales a toujours été un attribut de la souveraineté étatique [1094]. Des premières cartes topographiques aux systèmes d'information géographique contemporains, les États ont investi lourdement pour produire et contrôler ces données stratégiques, y voyant un gage d'autorité et de sécurité [1095]. La notion même de donnée géographique souveraine a été formalisée récemment en France. Il s'agit de données faisant référence sur le territoire national par leur qualité, leur fiabilité et leur caractère exhaustif, et dont la puissance publique entend garder la maîtrise. Cette maîtrise implique notamment de ne pas dépendre entièrement d'entités tierces pour accéder à des données géographiques critiques, et de ne pas fonder les décisions régaliennes sur des données dont l'État ne contrôlerait pas la chaîne de production et de validation.

Dans ce contexte, l'introduction de la blockchain peut apparaître comme une arme à double tranchant du point de vue de la souveraineté. D'un côté, elle offre aux États un outil puissant pour garantir l'intégrité de leurs registres fonciers, cartographiques ou stratégiques. En sécurisant les bases de données contre les manipulations et en renforçant la transparence, elle peut contribuer à consolider la confiance des citoyens dans les informations officielles. Le cas de la Géorgie illustre ainsi comment un gouvernement peut tirer parti d'une blockchain publique internationale (Bitcoin) pour améliorer la robustesse de son cadastre national. Ce faisant, la Géorgie a paradoxalement renforcé sa souveraineté foncière en luttant contre la corruption interne par un mécanisme technologique irrévocable, tout en s'appuyant sur une infrastructure technique globalisée qui échappe à son contrôle direct. De même, l'Estonie, en intégrant une blockchain à ses registres d'État, a accru sa résilience face aux cyberattaques et aux ingérences potentielles, et projette l'image d'un e-gouvernement souverain sur ses données, capable d'auditer toute action sur ses registres officiels. Ces exemples suggèrent que la blockchain, correctement gouvernée, peut être un vecteur de souveraineté numérique, en permettant à un État de garantir par la technique ce qu'il garantissait jusqu'alors par sa seule autorité juridique.

D'un autre côté, la nature distribuée et transnationale des blockchains soulève des interrogations géopolitiques. Ainsi, dans le cas d'un ancrage sur Bitcoin, par exemple, l'État dépend du bon

[1094] Valéria faure-Muntian, « Les données géographiques souveraines », Rapport au gouvernement, 2018, p. 3.
[1095] Ibid, p.12.

fonctionnement du réseau Bitcoin mondial, réseau dont la gouvernance échappe à tout État particulier et dont les acteurs sont répartis à travers le globe, et soumis à diverses juridictions. Une nation pourrait voir un élément critique de son infrastructure de données reposer sur une technologie dominée en pratique par des intérêts étrangers. Cette situation peut être jugée inconfortable du point de vue de la souveraineté classique. Divers conflits d'intérêt peuvent également surgir, si des données géographiques sensibles sont inscrites dans une blockchain publique, cela pourrait constituer une faille critique en cas de conflit dans une région où est hébergée une partie de la blockhain. Certes, la conception même d'un grand registre distribué est de ne dépendre d'aucun nœud unique, mais, en pratique, la concentration du pouvoir de calcul ou de développement peut créer des points de pression. De plus, même sans envisager des scénarios extrêmes, le simple fait d'utiliser une plateforme technologique externe peut aller à l'encontre de la doctrine de contrôle total des données souveraines.

Ainsi, en parallèle à ces développements, s'observe une tendance à la reterritorialisation des infrastructures blockchain pour les usages étatiques. L'Union européenne, par le biais du Partenariat européen de la Blockchain, travaille depuis 2018 à l'édification d'une infrastructure commune baptisée EBSI, où les nœuds seraient opérés par les États membres eux-mêmes[1096]. L'enjeu est de ne pas laisser le monopole des futurs grands registres distribués à des plateformes extraeuropéennes, et de s'assurer que les valeurs européennes soient inscrites dans le code de ces réseaux. De même, la France et d'autres pays investissent dans des solutions nationales ou des consortiums locaux, souvent en source ouverte, pour conserver la main sur la technologie. Le projet français de blockchain notariale (Blockchain d'Authentification des Documents officiels) ou la solution Tediji de Coexya sur Tezos s'inscrivent dans cette logique de souveraineté. La question de la souveraineté est donc de premier plan dans le développement de la blockchain.

La géopolitique des standards joue également un rôle clé. Si un protocole de blockchain géospatiale venait à s'imposer globalement, cela pourrait marginaliser les approches nationales qui n'y adhèrent pas. C'est pourquoi la France se doit de veiller à être présente dans les instances de normalisation internationales afin d'influer sur l'élaboration des standards de demain. Préserver une forme de souveraineté normative passe par cette diplomatie technique. Il s'agit de s'assurer que les formats de données, les protocoles d'interopérabilité, les mécanismes de sécurité intégrés aux blockchains correspondent aux intérêts et aux valeurs que l'on veut défendre. Par exemple, la notion d'« oracle » de confiance, indispensable pour relier les données du monde réel à la blockchain, pourrait faire l'objet de certifications ou d'agréments par les autorités publiques. Un État pourrait décider que seuls certains capteurs ou professionnels agréés peuvent injecter des données géographiques dans le

[1096] Commission européenne, « Infrastructure européenne de services Blockchain », 25 octobre 2024. https://digital-strategy.ec.europa.eu/fr/policies/european-blockchain-services-infrastructure. Consulté le 20 février 2025.

registre distribué national, et auditer ce processus. Ainsi, la blockchain ne supprime pas le rôle de l'État, mais le reconfigure en un rôle de surveillance et d'arbitrage de l'écosystème décentralisé.

Enfin, l'émergence de communautés auto-organisées de données géographiques (comme dans l'exemple de FOAM ou d'OpenStreetMap couplé à des solutions blockchain) pose la question de la légitimité de l'autorité cartographique. Si des citoyens, des entreprises, ou des ONG parviennent à créer des cartes fiables, certifiées par blockchain, indépendamment des canaux officiels, les gouvernements devront composer avec ces nouvelles sources de données. Cela peut être vu positivement, par exemple, en cas de catastrophe naturelle, une carte collaborative validée en temps réel par blockchain pourrait suppléer temporairement les bases officielles, mais aussi comme un défi à long terme : l'État doit-il intégrer, ignorer ou combattre ces registres alternatifs ? La souveraineté nationale sur la donnée géographique ne doit pas forcément tendre vers une forme d'autarcie, il peut s'agir également de s'assurer que, dans le concert des sources d'information, la source publique conserve un statut de référence et d'excellence, tout en étant capable d'évoluer en symbiose avec l'innovation externe. Dans cette perspective, la blockchain peut être un allié, en offrant des moyens de fédérer divers contributeurs autour d'un registre infalsifiable commun, ou un facteur de fragmentation, si, par exemple, plusieurs réseaux concurrents émergent, soutenus par des intérêts divergents.

En conclusion, l'intégration de la blockchain dans la certification de l'authenticité des données géographiques ne constitue pas une simple évolution technologique, mais bien un enjeu stratégique de souveraineté et de pouvoir. Elle invite à repenser le rôle de l'État comme garant de l'information territoriale à l'ère de la décentralisation informatique. Les expériences en cours, de la Géorgie à la Suède, de l'Estonie aux projets plus exploratoires, comme FOAM, démontrent un potentiel réel pour améliorer la fiabilité et la transparence des données géographiques. Cependant, elles rappellent aussi que la technologie s'insère dans un tissu sociopolitique existant qu'elle ne renverse pas instantanément. La blockchain ne rendra pas obsolètes les cadastres, les notaires, les géomètres ou les agences cartographiques, mais elle pourrait transformer leurs fonctions et les inciter à coopérer via de nouveaux modèles. Dans ce processus, chaque nation cherchera à défendre sa souveraineté sur ses données tout en participant à la construction d'une interopérabilité globale fiable, équilibre délicat entre ouverture et contrôle, caractéristique de la reconfiguration des rapports de pouvoir à l'ère du cyberespace. Les prochaines années verront sans doute se multiplier les cadres hybrides, les consortiums publics-privés et les traités d'interopérabilité autour de ces registres distribués, dans une dynamique où se joueront à la fois des intérêts économiques, des rapports de force géopolitiques et des idéaux de gouvernance ouverte.

L'ensemble de ces développements technologiques, qu'il s'agisse de la blockchain ou de l'intelligence artificielle, soulèvent des questions éthiques. Le rôle de l'État est parfois remis en

question, et l'impact potentiel de ces technologies sur la vie des citoyens ne peut être minimisé. La normalisation de ces technologies dans le domaine géospatial, est au cœur de ces développements, parce qu'elle constitue un vecteur essentiel de la diffusion de ces mêmes technologies.

1.3 Enjeux éthiques et réglementaires des nouvelles technologies

Les nouvelles technologies du cyberespace bouleversent ainsi les rapports de pouvoir et soulèvent des défis éthiques et réglementaires inédits. Dans le domaine des données géographiques numériques, ces transformations questionnent la souveraineté nationale et imposent de repenser les cadres normatifs à différentes échelles. Cette section vise à proposer une analyse approfondie de ces enjeux, articulée autour de cinq axes : les problématiques éthiques (vie privée, responsabilité, transparence algorithmique), les cadres juridiques (RGPD, AI Act, Data Act, droit foncier), les normes techniques et souverainetés juridiques (rôles de l'ISO, de l'OGC, du W3C, gouvernance du code), les enjeux géopolitiques et la diplomatie normative (cas de l'Union européenne, de la Chine, des États-Unis, de l'Estonie, etc.), et la dimension militaire (usages de l'IA et des données géospatiales à des fins militaires, éthiques de la guerre numérique).

Ainsi, les innovations technologiques actuelles s'accompagnent de problèmes éthiques majeurs, dont la protection de la vie privée, l'établissement de responsabilités claires et la transparence des algorithmes. L'intelligence artificielle et la collecte massive de données permettent des usages potentiellement intrusifs ou discriminatoires à grande échelle. Par exemple, il est démontré que l'IA « *permet d'accroître l'efficacité de certaines mesures discriminatoires qui existent déjà : profilage racial, prédiction de comportement, voire repérage de l'orientation sexuelle des personnes* » [1097], ce qui soulève d'importantes questions éthiques. La vie privée se trouve exposée tout au long du cycle de vie des systèmes numériques, nécessitant des cadres de protection robustes. L'UNESCO souligne ainsi que *« la vie privée doit être respectée, protégée et promue tout au long du cycle de vie des systèmes d'IA »*[1098], soulignant l'importance de mécanismes de sauvegarde des données personnelles à chaque étape. Dans le domaine géospatial, les données de localisation sont particulièrement sensibles : combinées à d'autres informations, elles offrent une *« visibilité sans précédent sur les activités, comportements et croyances »* [1099]des individus, ce qui menace potentiellement le respect des libertés fondamentales. Des initiatives éthiques comme la Locus Charter ont d'ailleurs émergé pour

[1097] Douglas M. David, Lacey Justine & Howard David, « Ethical risk for AI », AI Ethics, 2024. https://link.springer.com/article/10.1007/s43681-024-00549-9

[1098] UNESCO, Recommandation sur l'éthique de l'intelligence artificielle, Paris, 23 novembre 2021, § 32.

[1099] Ramos Gabriela, « Éthique de l'intelligence artificielle », UNESCO, 2024. https://www.unesco.org/fr/artificial-intelligence/recommendation-ethics

promouvoir un usage responsable des données de localisation [1100]. Un second enjeu éthique central concerne la responsabilité et l'équité des systèmes algorithmiques. Qui tient les rênes lorsque des décisions sont prises par des algorithmes opaques ? Les erreurs ou biais d'un système d'IA peuvent causer des torts réels, par exemple des discriminations dans l'accès à un service public, ou des accidents liés à un véhicule autonome, sans qu'il soit aisé d'en imputer la faute à un acteur identifié. Il s'agit ici du problème de la « boîte noire » algorithmique déjà évoqué précédemment. En effet, aujourd'hui, comme le soulignent les travaux de Cathy O'Neil et Frank Pasquale *« pour de nombreux consommateurs et régulateurs, les algorithmes ressemblent à des boîtes noires »* [1101], rendant difficile toute explication ou contestation des décisions automatisées [1102]. Cette opacité algorithmique mine la confiance et l'absence de transparence soulève d'importantes questions de responsabilité juridique et morale. En effet, comment garantir un recours effectif si l'on ne peut comprendre ni auditer le raisonnement de la machine ? Les principes d'explicabilité et de loyauté algorithmique sont ainsi devenus des impératifs éthiques largement reconnus dans la littérature et les guides de bonne conduite [1103]. Par ailleurs, des biais systématiques peuvent être introduits par des données d'entraînement non représentatives, conduisant l'algorithme à reproduire des discriminations sociales existantes. Les développeurs et les organisations se doivent aujourd'hui de rendre compte des effets de leurs algorithmes sur les individus et la société, et prévoir des mécanismes de contrôle humain appropriés.

Enfin, l'exigence de transparence est étroitement liée aux deux points précédents et constitue un principe transversal de l'éthique numérique. La transparence englobe la capacité des systèmes à expliquer leurs décisions, mais aussi la transparence institutionnelle quant aux finalités et méthodes de traitement des données. Ainsi, comme le rappelle un rapport de la CNIL, *« une entreprise ne peut se cacher derrière un algorithme pour éluder ses responsabilités »* [1104]. Des appels publics et politiques se multiplient pour réclamer plus de transparence autour des algorithmes utilisés notamment par les grandes plateformes numériques [1105]. Le respect de la vie privée, la prévention des biais discriminatoires et l'ouverture des « boîtes noires » algorithmiques sont ainsi devenus des invariants du

---

[1100] Kedar john, « Ethical Standards and Transparency Can Protect Location Data », Geospatial world, 2024. https://geospatialworld.net/prime/special-features/ethical-standards-and-transparency-can-protect-location-data/

[1101] Cathy O'Neil, « Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy », Crown Publishers, New York, 2016 ; voir également Frank Pasquale, « The Black Box Society: The Secret Algorithms that Control Money and Information », Harvard University Press, Cambridge, 2015, pp. 1–17.

[1102] Conseil de l'Europe, « Étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données et éventuelles implications réglementaires », DGI et MSI-NET, 2017, p. 41. https://rm.coe.int/algorithms-and-human-rights-fr/1680795681

[1103] Ibid, p 37.

[1104] CNIL, « Développement des systèmes d'IA : les recommandations de la CNIL pour respecter le RGPD », 8 avril 2024. https://www.cnil.fr/fr/developpement-des-systemes-dia-les-recommandations-de-la-cnil-pour-respecter-le-rgpd

[1105] Conseil de l'Europe, « Étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données et éventuelles implications réglementaires », DGI et MSI-NET, 2017, p. 41.

discours sur l'éthique des technologies. Face à ces défis, des organisations internationales et comités d'experts ont émis des lignes directrices. L'Union européenne, par exemple, via son groupe d'experts de haut niveau sur l'IA, promeut une IA digne de confiance basée sur sept exigences, dont la supervision humaine, la robustesse, la confidentialité des données et la transparence[1106]. De même, l'UNESCO a adopté en 2021 une Recommandation mondiale sur l'éthique de l'IA, fixant des valeurs et principes communs, et invitant les États à évaluer l'impact de ces systèmes sur les droits humains [1107]. Ces démarches illustrent la réponse normative éthique face aux innovations. Ainsi, la prise de conscience éthique est bien réelle. Cette dernière prépare le terrain à des évolutions réglementaires afin d'assurer un développement responsable de l'IA et des technologies numériques. Ainsi, les problématiques éthiques identifiées appellent l'élaboration de cadres juridiques adaptés. Les principes moraux doivent en effet se traduire en lois et régulations concrètes pour encadrer l'usage des nouvelles technologies.

Au-delà des lois formelles, la puissance des nouvelles technologies tient également aux normes techniques qui les sous-tendent. Formats de données, protocoles de communication, standards d'interopérabilité, autant de règles de facto qui structurent l'écosystème numérique mondial. Cependant, la définition de ces normes échappe souvent aux canaux étatiques traditionnels pour relever d'instances spécialisées, consortiums industriels ou communautés open source. Cette situation soulève un enjeu de souveraineté juridique et stratégique puisque celui qui contrôle les standards contrôle en partie l'évolution technologique et peut imposer ses préférences aux autres acteurs [1108].

Cet état de fait pose un double défi. D'une part, celui de la représentation des intérêts publics dans la définition des standards. En effet, si seuls des acteurs privés dominants élaborent les normes, il y a un risque que des considérations de concurrence ou de profit priment sur l'intérêt général. D'autre part, celui de la souveraineté : un État qui ne participe pas aux processus de standardisation peut se retrouver à appliquer des règles décidées ailleurs, éventuellement contraires à ses préférences. À l'inverse, l'implication dans ces instances peut être un levier d'influence. Conscients de cela, de plus en plus de gouvernements encouragent la présence de leurs experts dans les comités techniques internationaux et développent des stratégies de standardisation.

Un autre aspect crucial est la gouvernance du code source des logiciels et plateformes numériques. De plus en plus, les États réalisent que la maîtrise du logiciel est une composante de la

---

[1106] Commission européenne, Communication sur l'intelligence artificielle pour l'Europe, COM(2018) 237 final, 25 avril 2018 ; Groupe d'experts de haut niveau sur l'intelligence artificielle, Lignes directrices en matière d'éthique pour une IA digne de confiance, Bruxelles, 8 avril 2019.

[1107] UNESCO, « Recommandation sur l'éthique de l'intelligence artificielle », 2021. https://www.unesco.org/fr/legal-affairs/recommendation-ethics-artificial-intelligence

[1108] Seaman John, « China and the New Geopolitics of Technical Standardization », Ifri, 2020, p.7. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/seaman_china_standardization_2020.pdf

souveraineté numérique. Si les standards définissent quoi faire, le code implémente comment le faire. Dépendre de logiciels propriétaires étrangers pour des fonctions critiques peut exposer à des risques. C'est pourquoi certains gouvernements encouragent l'utilisation de logiciels libres et ouverts, dont le code peut être audité et modifié localement. L'Allemagne et la France voient ainsi l'open source comme un atout pour *« sécuriser [leur] identité numérique souveraine »*[1109]. Cela a été vu notamment avec des systèmes comme Linux, largement utilisés dans les administrations, où la communauté internationale du logiciel libre agit comme un organe de standardisation de fait, cependant les États y exercent aussi une influence via les contributions de leurs agences ou d'entreprises nationales. À l'inverse, l'absence d'accès au code peut mettre les États à la merci de décisions unilatérales des fournisseurs, comme souligné par de nombreux agents travaillant dans l'administration des bases de données géographiques sur le territoire. L'exemple du retrait brutal de Google API Maps il y a quelques années a sensibilisé nombre de collectivités locales à l'importance d'alternatives ouvertes pour les services de cartographie en ligne. Ainsi, la « gouvernance du code » recouvre l'ensemble des mécanismes par lesquels on encadre et oriente l'évolution des logiciels et algorithmes clés de l'écosystème numérique, que ce soit par des licences open source, des consortiums industriels, ou des politiques publiques de soutien à certaines technologies.

Ainsi, la bataille des standards techniques est devenue une bataille géopolitique et de souveraineté à part entière. Les normes et le code, souvent invisibles pour le grand public, tracent pourtant les frontières du possible dans le cyberespace. Assurer sa souveraineté, c'est donc non seulement légiférer, mais également investir les arènes de normalisation technique. L'influence normative peut agir comme une composante du Soft Power des États. À titre d'exemple, l'Europe essaie d'imposer ses valeurs via des standards ouverts et respectueux des droits humains, via l'intégration de considérations d'accessibilité, de durabilité ou d'éthique dans les normes ISO[1110]. À l'inverse, d'autres puissances peuvent chercher à imposer des standards avantageant leurs champions industriels ou permettant un meilleur contrôle de l'information. Les nouvelles technologies numériques, en redéfinissant les flux d'information et la maîtrise des données, participent à une reconfiguration des rapports de pouvoir à l'échelle internationale. Dès lors, elles deviennent un terrain d'affrontement géopolitique et un objet de diplomatie normative. Les États et ensembles régionaux cherchent à promouvoir leurs propres règles du jeu dans le cyberespace, que ce soit via des lois, des standards ou des initiatives de coopération. Ainsi, émergent aujourd'hui divers modèles de souveraineté

[1109] Tranberg Pernille, « Open Source – One Path to Digital Sovereignty », data Ethics, 28 juin 2024. https://dataethics.eu/open-source-one-path-to-digital-sovereignty/. Consulté le 10 juillet 2024.

[1110] Seaman John, « China and the New Geopolitics of Technical Standardization », Ifri, 2020, p.7. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/seaman_china_standardization_2020.pdf

numérique concurrents, portés notamment par l'Union européenne, la Chine et les États-Unis, tandis que des pays plus petits comme l'Estonie innovent pour exister dans ce paysage.

L'Union européenne s'est imposée ces dernières années comme un exportateur de normes ambitieux, aspirant à jouer un rôle de régulateur global du numérique. Ce phénomène, qualifié d'« effet de Bruxelles », repose sur le poids économique de l'UE et son choix de régulations strictes qui finissent par s'imposer aux acteurs mondiaux [1111]. L'exemple du RGPD qui a déjà été évoqué a eu un effet d'entraînement planétaire. L'UE tente de reproduire ce schéma avec l'AI Act (cadre IA) et d'autres textes (Digital Services Act, Digital Markets Act pour la régulation des plateformes, Data Governance Act, etc.), cherchant à définir une troisième voie technologique fondée sur la primauté des droits de l'homme, la concurrence équitable et la protection du consommateur, en contraste à la fois avec le laisser-faire américain et le contrôle étatique chinois [1112]. Cette diplomatie normative européenne s'inscrit dans une vision stratégique de souveraineté numérique. La Commission européenne affiche clairement l'objectif de *« renforcer sa souveraineté dans la décennie numérique »*[1113], en investissant dans des capacités propres (microprocesseurs européens, cloud Gaia-X, réseau 5G sécurisée, constellations de satellites comme Galileo). Sur la scène internationale, l'UE promeut ses standards via des forums multilatéraux (ONU, UIT, UNESCO) et des accords bilatéraux. Par exemple, l'UE a conclu avec le Japon, la Corée du Sud ou le Canada des partenariats sur l'IA et la data qui encouragent l'adoption de principes proches des siens. La diplomatie normative européenne se manifeste aussi par des discours sur la « souveraineté numérique européenne » et la nécessité de défendre un Internet ouvert, libre et sécurisé sur la base du droit international. En 2018, la France a lancé avec soutien européen l'« Appel de Paris pour la sécurité et la confiance dans le cyberespace »[1114], appel à la coopération internationale pour poser des normes de comportement étatique responsable dans le cyberespace. L'UE mise donc sur son pouvoir réglementaire et sa force de marché pour façonner l'ordre numérique mondial selon ses valeurs. Toutefois, cette approche n'est pas sans résistances. Les États-Unis et la Chine, notamment, ne se conforment pas spontanément aux régulations européennes, cherchant plutôt à imposer les leurs ou à contester celles de l'UE en instance de normalisation internationale. Malgré cela, on constate que, plutôt que de développer des processus séparés, beaucoup

---

[1111] Bradford Anu, « The Brussels Effect : How the European Union Rules the World », Oxford University Press, 2020, pp. 833-838.; Meyer Zach, « In tech, the death of the Brussels effect is greatly exaggerated », 8 décembre 2023. https://www.cer.eu/insights/tech-death-brussels-effect-greatly-exaggerated#. Consulté le 15 janvier 2024.

[1112] Isaac Henri, « Quelle souveraineté numérique européenne ? », in Revue française de gestion, n° 305, 22 août 2022, pp. 63-77.

[1113] Communication de la Commission au parlement européen, au conseil, au Comité économique et social européen et au Comité des régions, « Une boussole numérique pour 2030: l'Europe balise la décennie numérique », COM(2021) 118 finals, Bruxelles, 9 mars 2023. Disponible ici : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021DC0118. Consulté le 15 février 2024.

[1114] https://pariscall.international/fr/

d'entreprises mondiales se conforment aux règles européennes du fait de l'importance incontournable du marché UE. Cela confère à l'Europe une influence bien réelle.

La Chine, de son côté, promeut un modèle alternatif souvent résumé par le concept de « souveraineté cybernétique » (Internet sovereignty). Beijing défend l'idée que chaque État doit avoir le contrôle absolu sur le segment de l'Internet présent sur son territoire, y compris en matière de filtrage des contenus et de choix des infrastructures. Ce principe s'oppose à la vision occidentale d'un Internet global, ouvert et multiacteur. La posture chinoise se concrétise en interne par le Grand Firewall (système de censure et de contrôle du trafic Internet chinois) et l'écosystème technopolitique de surveillance (caméras à reconnaissance faciale, systèmes de crédit social, etc.)[1115]. Sur la scène internationale, la Chine conteste le modèle multipartite de gouvernance de l'Internet, dominé par des organisations comme l'ICANN, l'IETF ou le W3C, où les gouvernements n'ont pas le monopole des décisions. Elle préconise un rôle plus central pour des instances intergouvernementales, comme l'UIT où chaque État dispose d'une voix égale. Dans ce cadre, la Chine a proposé des évolutions majeures de l'architecture Internet, comme la proposition de « New IP » [1116]ou celle de renforcement des capacités de contrôle sur l'IPv6 [1117]. Ces initiatives suscitent de fortes inquiétudes en Occident, où elles sont perçues comme une tentative d'institutionnaliser une sorte de « splinternet » : un Internet fragmenté en zones d'influence nationales, au risque de briser l'interopérabilité globale et d'instaurer des normes autoritaires. La stratégie chinoise passe aussi par le plan China standards 2035, qui vise à accroître la présence chinoise dans les organismes internationaux de standardisation dans les domaines émergents. Beijing joue ici un jeu subtil, et cherche à la fois s'engager dans les instances existantes en y plaçant ses experts, et en parallèle à créer ses propres cadres bilatéraux ou régionaux pour ses standards via les routes de la soie numériques. Par le biais d'accords dans le cadre de la BRI (Belt and Road Initiative), la Chine exporte ses technologies et ses normes techniques dans de nombreux pays d'Asie, d'Afrique et d'Amérique latine. Cela lui permet de diffuser son modèle et de gagner en influence normative.

Les États-Unis, quant à eux, ont historiquement dominé l'espace numérique, tant sur le plan des infrastructures que des grands acteurs privés comme les GAFAM. Leur approche a longtemps été marquée par un libéralisme technologique, laisser le secteur privé innover avec un minimum de régulation, et par la promotion d'un Internet ouvert conforme aux valeurs américaines de liberté d'expression et de libre entreprise. Sur le plan géopolitique, cela s'est traduit par la défense du modèle

---

[1115] Zúñiga Nicholas , Burton Datta Saheli , Blancato Filippo, Carr Madeline, « The geopolitics of technology standards: historical context for US, EU and Chinese approaches », in *International Affairs*, Vol. 100, n°4, Juillet 2024, pp. 1635–1652. https://academic.oup.com/ia/article/100/4/1635/7692873. Consulté le 4 mars 2025.

[1116] Ibid.

[1117] Yin Jessie, « The Race for Cyberspace: China's IP Standards and the Threat to Net Neutrality », china observer, 10 octobre 2024. https://chinaobservers.eu/the-race-for-cyberspace-chinas-ip-standards-and-the-threat-to-net-neutrality/. Consulté le 4 avril 2025.

multipartite de la gouvernance Internet, impliquant la société civile, les experts techniques et les entreprises aux côtés des États, plutôt qu'un contrôle onusien strict. Les États-Unis ont ainsi soutenu l'ICANN indépendant pour la gestion des noms de domaine, avant de s'en détacher officiellement en 2016 sous la présidence Obama, et se sont opposés aux tentatives de reprendre la gouvernance d'Internet au niveau de l'UIT. Cependant, l'hégémonie technologique américaine a aussi été utilisée comme un instrument de pouvoir. Ainsi, outre le Cloud Act déjà mentionné qui applique extraterritorialement le droit US via les entreprises américaines, il faut mentionner les révélations Snowden en 2013 qui ont montré comment la NSA exploitait les infrastructures globales pour la surveillance mondiale. En réponse à la montée de la Chine, les États-Unis ont récemment adopté une posture plus proactive en matière de diplomatie technologique. Ils ont lancé en 2020 l'Initiative Clean Network[1118] pour convaincre les pays alliés d'exclure les équipements chinois de leurs réseaux 5G, et ont établi en 2020 une Initiative mondiale pour la gouvernance des données visant à promouvoir des principes de libre circulation des données avec confiance. Washington mise aussi sur ses alliances. Par exemple, le dialogue UE–USA sur la technologie, le Trade and Technology Council, vise à harmoniser les approches sur l'IA, les semiconducteurs et les plateformes en ligne, afin de contrer les modèles opposés. Il y a donc un clair enchaînement géopolitique où les tensions entre grandes puissances se projettent dans le cyberespace sous forme de guerre normative et de guerre d'influence. Ainsi, si les États-Unis conservent des atouts majeurs, ils doivent désormais tenir compte de la régulation européenne d'une part et de la percée technologique chinoise d'autre part.

Dans ce paysage dominé par les grandes puissances, des plus petits États parviennent aussi à innover et à peser au-delà de leur taille, en jouant la carte de l'audace normative ou technologique. L'Estonie en offre un exemple remarquable. L'Estonie a misé très tôt sur le numérique pour renforcer sa souveraineté après la Guerre froide, avec l'adoption dès 1994 du premier schéma stratégique « Principes de la politique d'information estonienne » octroyant 1% du PIB aux nouvelles technologies, suivie du lancement en 1994 de l'initiative « Tiger Leap » (Saut du Tigre) visant à équiper toutes les écoles du pays en ordinateurs et à connecter à termes l'ensemble de la population à Internet[1119]. Elle a ainsi construit une « e-administration » avancée et lancé le programme d'« e-Residency » permettant à des entrepreneurs étrangers d'obtenir une identité numérique estonienne pour créer des entreprises dans l'UE[1120]. L'Estonie a également innové sur le plan conceptuel avec l'idée d'« ambassade de données » (data embassy). En 2017, elle a ouvert au Luxembourg la première « ambassade numérique » au monde

[1118] Dąbrowski Andrzej, « The Clean Network Initiative as an Element of the U.S.-China Competition »,PISM Polski Instytut Spraw Międzynarodowych, 2021. https://www.ceeol.com/search/gray-literature-detail?id=1164684

[1119] Terriou Louis, « Estonie : la société numérique la plus avancée du monde ? », Regard sur l'Est, 11 avril 2023

[1120] Republic of Estonia, « Why Estonia offers e-Residency », 2 mars 2025. https://learn.e-resident.gov.ee/hc/en-us/articles/360000720437-Why-Estonia-offers-e-Residency. Consulté le 4 mai 2025.

qui constitue un centre de données hors du territoire estonien, mais placé sous juridiction estonienne, abritant des copies sauvegardées des registres critiques de l'État[1121]. Cette solution vise à assurer la continuité de l'État en cas de cyberattaque massive ou même d'invasion militaire du territoire, une menace que l'Estonie prend au sérieux compte tenu du contexte géopolitique. L'Estonie a ainsi redéfini la souveraineté en la dissociant du territoire physique, ses citoyens pourraient continuer à accéder aux services gouvernementaux même si le sol national était occupé, grâce à ces doubles numériques à l'étranger. Cette initiative a inspiré d'autres pays, comme le Luxembourg, qui a lui-même légiféré pour accueillir des data embassies, d'autres envisagent de tels accords[1122]. Ainsi, par son dynamisme diplomatique, l'Estonie a su valoriser son expertise. Elle accueille le Centre de cybersécurité de l'OTAN (CCDCOE) qui publie le célèbre Manuel de Tallinn sur le droit international applicable au cyberespace, et elle pèse dans les débats onusiens sur les cyberconflits. De plus, l'Estonie milite pour l'adoption de standards d'interopérabilité gouvernementale, comme X-Road, sa plateforme d'échange de données. Ainsi, le cas de l'Estonie illustre comment un petit État peut développer une véritable stratégie de diplomatie normative. Selon l'analyse de Pierre-Marie Dupuy (1992)[1123], la diplomatie normative se caractérise par un effet cumulatif où la répétition des sollicitations normatives place les États dans une posture défensive vis-à-vis de leurs engagements internationaux. Cette diplomatie normative n'est d'ailleurs par l'apanage des États. Comme le montre Ali Kairouani (2020), les grandes entreprises la pratiquent aussi, soit directement, soit en proposant leurs propres standards dans les instances multilatérales de normalisation, soit indirectement par l'intermédiaire de leurs fédérations professionnelles et avec l'appui de leurs gouvernements[1124]. Le cas de l'Estonie illustre très bien comment un État peut, en excellant dans un domaine, ici la gouvernance numérique, influencer des normes internationales et assurer le développement de standards internationaux renforçant sa propre souveraineté. Parmi les autres exemples notables de diplomatie normative, pourrait être cité un pays comme l'Inde, qui développe sa propre vision de souveraineté numérique, notamment via la localisation des données et des infrastructures critiques nationales, tout en s'affirmant comme porte-parole des pays en développement sur ces questions [1125], ou encore les initiatives de blocs régionaux,

---

[1121] Robinson Nick, Kask Laura, Krimmer Robert, « The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis », ICEGOV '19: Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, 3 avril 2019. https://dl.acm.org/doi/abs/10.1145/3326365.3326417. Consulté le 22 janvier 2024.

[1122] Ibid.

[1123] P.-M. Dupuy, Droit international public, Paris, Dalloz, 1992, p. 264.

[1124] KairouaniAli, « Le pouvoir normatif des entreprises multinationales en droit international », Revue internationale de droit économique, t. XXXIV, 2020/3, pp. 253 – 295.

[1125] Vila Seoane, M. F., « Data sécurisation: the challenges of data sovereignty in India », in *Third World Quarterly*, 42(8), 2021, pp. 1733–1750. https://doi.org/10.1080/01436597.2021.1915122. Consulté le 18 août 2024.

comme l'Union africaine, qui ont adopté en 2014 une Convention sur la cybersécurité et la protection des données personnelles, dite Convention de Malabo[1126].

Cependant, les divergences de vues sur la gouvernance du cyberespace se manifestent jusque dans les enceintes multilatérales, par exemple, à l'ONU, deux forums parallèles, l'Open-Ended Working Group, soutenu par la Russie et la Chine, et le Group of Governmental experts, soutenus par les Occidentaux, ont longtemps travaillé en parallèle sur les normes de comportement des États dans le cyberespace, révélant des visions disjointes. La diplomatie normative est donc devenue un champ de la géopolitique contemporaine. Édicter la règle du jeu numérique permet d'étendre sa sphère d'influence. L'Union européenne est souvent présentée comme le « régulateur du monde », la Chine comme le champion de la souveraineté étatique absolue en ligne, les États-Unis comme le gardien d'un Internet libre, mais dominé par ses entreprises, et des pays comme l'Estonie comme des laboratoires offrant de nouvelles perspectives. Cette concurrence normative n'est pas sans conséquences, elle pourrait aboutir à un Internet fragmenté en régimes juridiques distincts, entraînant une forme de balkanisation du cyberespace, ou au contraire, pousser vers l'adoption de dénominateurs communs. Toujours est-il que le facteur technologique est désormais au cœur de la puissance des nations. La souveraineté nationale se mesure aussi à la capacité d'un État à protéger ses données, à réguler les plateformes étrangères sur son sol, à fournir à ses citoyens des services numériques sécurisés, et à imposer ou négocier ses standards à l'étranger. Une dimension où cet aspect est particulièrement critique est celle de la défense et de la sécurité.

Le domaine militaire constitue un laboratoire pour les nouvelles technologies, tant les promesses y sont grandes et les conséquences potentiellement importantes. L'IA, la robotique autonome, le traitement massif de données géospatiales, la guerre cybernétique, sont autant d'innovations qui transforment l'art de la guerre et posent d'importantes questions éthiques et juridiques. Le poids des nouvelles technologies dans la puissance militaire est devenu tel qu'il reconfigure lui aussi les rapports de force internationaux. Un aspect crucial est l'exploitation des données géospatiales et de la surveillance. La maîtrise de l'information géographique a toujours été un atout militaire. Aujourd'hui, grâce aux satellites d'observation, aux drones, aux capteurs au sol et à l'IA, les armées disposent de quantités massives de données en temps quasi réel sur les théâtres d'opérations. Sur le terrain, l'intégration de capteurs et d'IA confère une supériorité informationnelle décisive, comme cela a été illustré durant le conflit du Haut-Karabagh en 2020 entre l'Arménie et l'Azerbaïdjan ou en Ukraine depuis 2022, où les drones de reconnaissance et les images satellites

[1126] Union Africaine, « Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel », 23e session ordinaire de la conférence de l'Union, Malabo, 27 juin 2014. https://www.afapdp.org/wp-content/uploads/2018/06/CONV-UA-CYBER-PDP-2014.pdf. Consulté le 11 avril 2025.

commerciales fournies par des entreprises privées ont aidé au ciblage et à la connaissance de la situation en temps réel.

Les données géospatiales sont également au cœur des systèmes de navigation et de positionnement essentiels aux opérations militaires. L'enjeu de souveraineté ici se traduit par la volonté d'indépendance vis-à-vis du GPS américain. L'Europe a développé Galileo précisément pour ne pas dépendre uniquement du GPS pour ses forces armées. Galileo est vu comme un outil emblématique d'autonomie stratégique offrant une alternative sous contrôle européen, depuis le lancement des premiers satellites en 2011 [1127]. Il fournit un service sécurisé dont pourront bénéficier les armées européennes en parallèle du signal GPS. Au-delà de l'aspect technique, Galileo a été un projet éminemment politique, en effet, les États-Unis s'y sont d'abord opposés, craignant qu'il brouille les signaux ou offre aux adversaires un système de rechange. Les Européens ont tenu bon au nom de la souveraineté, révélant une prise de conscience de l'importance de maîtriser ces infrastructures spatiales et de navigation. En cas de crise majeure, un pays ne peut se permettre d'être coupé d'un système de positionnement par la décision d'un autre État, d'où l'importance de systèmes comme Galileo. Par ailleurs, les armées ont développé des systèmes multiconstellation capables d'exploiter à la fois GPS et Galileo pour assurer redondance et robustesse, comme le système français P3TS, décrites comme une solution souveraine combinant signaux Galileo et GPS afin d'allier performance et indépendance par le ministère des armées[1128].

Ainsi, dans le cyberespace, les données géographiques numériques ne sont plus de simples outils ou ressources neutres, ils sont devenus des enjeux de pouvoir à part entière. Les principes fondateurs de l'ordre international sont réinterprétés à l'aune du numérique. Désormais, un pays souverain doit pouvoir contrôler ses données, ou tout du moins leur usage sur son sol, fixer des règles pour les acteurs technologiques opérant sur son territoire, participer à la définition des normes globales qui structureront les infrastructures de demain, et protéger ses intérêts dans les espaces nouveaux que sont le cyberespace et l'espace infogéographique. Les problématiques éthiques ont initialement sonné l'alarme, poussant à une prise de conscience des risques. Cela a conduit à l'édiction de cadres juridiques novateurs, en particulier sous l'impulsion de l'Union européenne, qui tente de concilier innovation technologique et droits fondamentaux. Parallèlement, la question des normes techniques s'est imposée comme un front moins visible, mais tout aussi crucial, où se jouera la liberté d'action des États, car dominer les standards, c'est dicter en partie l'avenir technologique. Sur la scène

---

[1127] Darnis Jean-Pierre, « Sécurité et défense spatiale de l'Union européenne », in *L'Année de la Défense nationale - Ruptures stratégiques. Quels enjeux pour la France et pour l'Europe ?*, la documentation française, 2024. https://shs.cairn.info/article/LDF_DURIEU_2024_01_0115

[1128] P3TS - "Plug and Play Positioning and Timing System", 2024. https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-armes/p3ts-plug-and-play-positioning-and-timing-system. Consulté le 31 août 2025.

internationale, se déploie une véritable diplomatie normative, chaque grand acteur exportant sa vision de l'espace numérique. L'UE se positionne en championne d'un Internet réglementé et éthique, la Chine en héraut de la souveraineté étatique et du contrôle, les États-Unis en défenseur d'un modèle libéral centré sur ses entreprises, pendant que des pays comme l'Estonie prouvent qu'intelligence numérique et souveraineté peuvent se renforcer mutuellement, quelle que soit la taille du pays.

Se dégagent ainsi plusieurs tendances de fond. Tout d'abord, une tendance à la reterritorialisation du cyberespace. Après l'utopie d'un Internet sans frontières régulé par lui-même, on voit les États réaffirmer leur rôle, que ce soit en construisant des murs numériques ou en projetant leur loi au-delà de leurs frontières. Enfin, il apparaît que la souveraineté nationale à l'ère du numérique ne peut plus se penser de manière isolée. Cette dernière est forcément enchâssée dans des cadres plus larges (régionaux, internationaux) et nécessite une coordination. En conclusion, les nouvelles technologies imposent aux États un changement de paradigme, leur pouvoir ne repose plus uniquement sur la maîtrise d'un territoire physique, mais aussi sur la capacité à maîtriser l'espace informationnel et normatif. Ceux qui sauront s'adapter, innover et coopérer auront l'avantage dans la reconfiguration en cours des rapports de pouvoir. La France, à travers la question de la standardisation des données géographiques numériques, a là un défi et une opportunité. Il lui faudra mobiliser son savoir-faire géospatial, juridique et diplomatique pour assurer que le cyberespace, nouvelle frontière de la souveraineté, reste conforme à ses intérêts et à ses valeurs.

Au terme de cette première section consacrée à l'intelligence artificielle et à la blockchain comme nouveaux terrains de la normalisation, plusieurs constats s'imposent qui éclairent les développements à venir. L'analyse des standards de données sémantiques, tels que JSON-LD, GeoJSON-LD et GeoSPARQL, a démontré l'existence d'une infrastructure normative sans laquelle le potentiel de l'intelligence artificielle appliquée aux données géographiques ne pourrait être pleinement exploité. Ces formats constituent désormais le langage commun permettant aux algorithmes d'apprentissage automatique de « comprendre » l'information territoriale, de réduire les ambiguïtés lors des intégrations de données et d'assurer la base technique sur laquelle se construisent les applications intelligentes de la géomatique contemporaine. L'examen des applications de l'IA géospatiale, tant civiles que militaires, a montré l'ampleur des transformations en cours, mais aussi les défis éthiques qu'elles soulèvent : biais algorithmiques, opacité des « boîtes noires », menaces sur la vie privée, dilution des responsabilités. L'analyse de la blockchain a révélé son potentiel pour certifier l'authenticité et l'intégrité des données géographiques dans un contexte où la manipulation de l'information territoriale devient un enjeu de guerre informationnelle, tout en soulignant ses limites (dépendance à la qualité des données initiales, tension avec le droit à l'oubli du RGPD, nécessité d'adaptations législatives). Enfin, l'examen des enjeux éthiques et réglementaires a mis en lumière

l'émergence de modèles concurrents de diplomatie normative, dont la confrontation structure désormais la gouvernance mondiale des technologies numériques.

Ces différents éléments, analysés séparément, ne prennent cependant leur pleine signification que lorsqu'ils sont mis en cohérence dans des systèmes intégrés capables de représenter, de simuler et d'interagir avec le territoire dans toutes ses dimensions. C'est précisément cette synthèse qu'opèrent les jumeaux numériques territoriaux et les métavers géographiques, dont l'essor constitue l'une des transformations les plus significatives de la géomatique contemporaine. Un jumeau numérique territorial ne peut fonctionner sans mobiliser simultanément l'ensemble des composantes précédemment analysées. En effet, il repose sur des données géospatiales structurées selon les standards de l'OGC et de l'ISO, exploite l'intelligence artificielle pour analyser et prédire l'évolution du territoire, peut intégrer des mécanismes de certification blockchain pour garantir l'intégrité des informations critiques, et demeure soumis aux mêmes exigences éthiques et réglementaires de protection des données personnelles, de transparence algorithmique et de contrôle humain. Les métavers géographiques ajoutent à cette architecture une couche d'interaction homme-machine qui démultiplie les possibilités d'usage, de la concertation urbanistique en réalité virtuelle à la gestion de crises en temps réel.

Cette intégration amplifie considérablement les enjeux de normalisation identifiés dans les sections précédentes. Un jumeau numérique urbain doit assembler des données provenant de sources multiples et hétérogènes, dont la compatibilité suppose une normalisation rigoureuse à tous les niveaux. Les environnements immersifs posent ainsi des défis supplémentaires. Les différentes plateformes de réalité augmentée utilisent des approches propriétaires peu interopérables, et la bataille entre formats ouverts et formats propriétaires, déjà analysée pour les données géospatiales classiques, se rejoue dans l'univers des métavers. Par ailleurs, la dialectique entre ouverture et contrôle se retrouve amplifiée. L'ouverture est nécessaire pour permettre l'assemblage de données provenant de multiples acteurs, mais elle expose les jumeaux numériques pilotant des infrastructures critiques à des risques de manipulation dont les conséquences pourraient se traduire dans la réalité territoriale. La question de la confiance, centrale dans l'analyse de la blockchain, devient une condition sine qua non de l'adoption de ces technologies par les acteurs territoriaux. La dimension géopolitique, enfin, traverse l'ensemble de ces problématiques. En effet, qui définira les standards des jumeaux numériques et des métavers contrôlera une part significative des représentations virtuelles du territoire, enjeu de souveraineté par excellence.

C'est l'ensemble de ces questions que la partie suivante se propose d'examiner, en analysant successivement les infrastructures normatives des jumeaux numériques territoriaux, les défis de l'interopérabilité dans les environnements de réalité augmentée, et les cybermenaces spécifiques qui

pèsent sur ces systèmes où toute faille informatique peut avoir des répercussions concrètes sur le fonctionnement du territoire.

2. L’essor des jumeaux numériques et des métavers géographiques

L’émergence conjointe des jumeaux numériques territoriaux et des métavers géographiques transforme en profondeur le champ de la géomatique. Ces innovations reposent sur la capacité à représenter et à gérer des données spatiales massives et multidimensionnelles de manière cohérente. Elles soulèvent également de nouveaux enjeux en matière de normalisation des données géographiques, d’interopérabilité entre systèmes, et de cybersécurité des environnements immersifs.

2.1 Normalisation des infrastructures de jumeaux numériques territoriaux

Comme souligné précédemment, le jumeau numérique territorial se définit comme une réplique numérique dynamique d’un espace géographique, alimentée par des données géolocalisées en temps réel. Pour déployer de tels jumeaux à l’échelle des territoires, la normalisation des données et des infrastructures est cruciale. En effet, sans standards communs, les données géospatiales hétérogènes (cartographie 2D, modèles 3D, capteurs IoT, etc.) risquent de demeurer silotées, compromettant l’intégration cohérente des informations. Des efforts internationaux émergent afin de doter les jumeaux numériques de bases standardisées. À titre d’exemple, la Corée du Sud a établi des standards nationaux en s’appuyant sur les normes existantes de l’information géographique et sur le standard OGC CityGML 3.0 pour définir des modèles de données 3D interopérables pour chaque domaine territorial [1129]. CityGML, standard ouvert de l’OGC, fournit en effet un schéma sémantique commun pour représenter les objets urbains en trois dimensions (bâtiments, voiries, réseaux) avec leurs attributs géométriques et thématiques [1130]. L’adoption de tels standards géospatiaux assure que les différentes composantes du jumeau puissent être combinées et échangées sans perte d’information.

En parallèle, d’autres normes ouvertes complètent l’écosystème des jumeaux numériques. On peut citer SensorThings API de l’OGC pour intégrer les données de capteurs en temps réel, IndoorGML pour la cartographie des espaces intérieurs, ou encore 3D Tiles pour la diffusion Web de modèles 3D volumineux[1131]. L’ensemble de ces standards s’inscrit souvent dans le prolongement des Infrastructures

[1129] Seunghun Kang, « Use Case of National Digital Twin Standard for Buildings », FIG Working Week,Your World, Our World: Resilient Environment and Sustainable Resource Management for all Accra, Ghana, 19–24 mai 2024. https://www.fig.net/resources/proceedings/fig_proceedings/fig2024/papers/ts10b/TS10B_seunghun_12547_abs.pdf. Consulté le 2 mars 2025, p. 4.

[1130] Sarafinof Dimitri, Servant Fabrice, Rönsdorf Carsten et al., « Urban Digital Twins: Integrating Infrastructure, natural environment and people », OGC Discussion paper, p. 10, 2024. https://docs.ogc.org/dp/24-025.html. Consulté le 12 mars 2025.

[1131] Pear Channing, « Top 5 Interoperability Standards for Digital Twins », Anvil Labs, 24 février 2025. https://anvil.so/post/top-5-interoperability-standards-for-digital-twins#. Consulté le 15 mars 2025.

de Données spatiales (IDS), étendues aux dimensions 3D et temporelles. L'OGC promeut d'ailleurs une vision du Urban Digital Twin (UDT) comme plateforme d'interopérabilité des données urbaines, s'appuyant sur une panoplie de normes ouvertes couvrant SIG, BIM, simulations, analyses IoT, etc.[1132]. Comme le résume un document de l'OGC, un jumeau numérique urbain peut être envisagé comme *« une représentation virtuelle d'une ville dynamique qui permet aux utilisateurs d'exploiter les interrelations entre les infrastructures physiques, l'environnement naturel et les habitants à l'échelle d'une ville »*[1133]. Dans cette optique, les normes ouvertes sont essentielles. Leur usage garantit l'interopérabilité et la pérennité des systèmes, en évitant l'enfermement propriétaire. De fait, les normes ouvertes seront essentielles au succès du métavers et des jumeaux numériques, note l'OGC, soulignant que pratiquement *« n'importe quelle norme géospatiale 3D sera utile pour construire le métavers »*[1134]. Autrement dit, la normalisation géographique offre le socle commun sans lequel l'essor des jumeaux numériques territoriaux serait freiné.

En insistant sur une rigueur cartographique et sur des modèles de données unifiés, la normalisation facilite l'assemblage de jumeaux numériques multiéchelles. Ainsi, un jumeau numérique de ville peut intégrer à la fois des maillages 3D détaillés des bâtiments, des données sociodémographiques localisées par quartier, et des informations environnementales (bruit, qualité de l'air) en temps réel, à condition que tous ces jeux de données respectent des standards compatibles. Dans l'Union européenne, des initiatives comme la directive INSPIRE ont préparé le terrain en harmonisant les référentiels géographiques, tandis que des extensions vers la 3D/4D sont en cours pour appuyer les smart cities et leurs jumeaux numériques. Cette démarche de normalisation permet non seulement l'échange fluide de données entre acteurs (collectivités, opérateurs, chercheurs), mais aussi le développement d'outils génériques réutilisables d'un territoire à l'autre. À terme, un métavers territorial s'appuyant sur ces normes pourrait offrir une représentation numérique complète du territoire, servant de support à la concertation urbanistique, aux simulations de politiques publiques ou à la gestion de crises en temps réel. Cependant, pour atteindre cette vision, un défi de taille consiste à assurer l'interopérabilité entre les multiples plateformes et technologies impliquées.

[1132] Sarafinof Dimitri, Servant Fabrice, Rönsdorf Carsten et al., « Urban Digital Twins: Integrating Infrastructure, natural environment and people », OGC Discussion paper, p. 8, 2024. https://docs.ogc.org/dp/24-025.html#. Consulté le 12 mars 2025.

[1133] Ibid.

[1134] Chester Simon, « Le métavers est géospatial », OGC, article de blog, 3 mai 2022. https://www.ogc.org/fr/blog-article/the-metaverse-is-geospatial/#. Consulté le 24 novembre 2024.

2.2 Défis de l'interopérabilité et des réalités augmentées

L'interopérabilité est souvent décrite comme *« l'essence même du concept »*[1135] de métavers, tant la promesse de ces mondes numériques repose sur la continuité entre différentes plateformes, applications et expériences. Dans le contexte de l'exploitation des données géographiques, le concept d'interopérabilité revêt plusieurs dimensions imbriquées. D'un point de vue technique, il s'agit d'abord de faire communiquer des systèmes variés, SIG 3D, applications de réalité augmentée (RA), simulateurs en réalité virtuelle, bases de données spatiales, en assurant la compatibilité des données et des protocoles. Mais l'interopérabilité s'entend aussi aux niveaux matériels (casques, capteurs, smartphones aux systèmes variés), logiciels (moteurs 3D, SDK AR différents), sémantiques (modèles 3D et ontologies spatiales divergents) et même au niveau des interfaces d'interaction pour l'utilisateur. Assurer la cohérence à tous ces niveaux est un défi majeur pour l'essor d'un métavers géographique unifié.

La réalité augmentée illustre particulièrement ces défis. Elle consiste à superposer des contenus virtuels géoréférencés à la perception du monde réel, ce qui requiert une correspondance spatiale précise entre les deux. Différentes plateformes RA comme l'ARKit d'Apple, l'ARCore de Google, ou encore l'HoloLens de Microsoft, utilisent aujourd'hui des approches propriétaires, créant une profusion de « normes de facto » peu interopérables. Un même objet virtuel pourra apparaître positionné différemment selon les systèmes si les référentiels ne coïncident pas. De plus, la pérennité des contenus RA pose question : comment garantir qu'une annotation géolocalisée réalisée dans une application pourra être vue par un autre utilisateur via une application différente ? Sans standardisation, chaque silo applicatif constitue un îlot séparé dans le métavers naissant. Cependant, plusieurs initiatives cherchent donc à établir des standards d'interopérabilité pour la RA. L'OGC ARML 2.0 (Augmented Reality Markup Language), par exemple, permet de décrire des objets virtuels dans une scène RA, en spécifiant leur apparence et surtout leur ancrage géographique dans le monde réel [1136]. Ce standard fournit un langage commun pour que des applications différentes partagent des Points d'Intérêt virtuels avec leurs coordonnées. De même, la norme OGC GeoPose définit un format universel pour échanger la position et l'orientation d'un objet ou d'un utilisateur dans l'espace géodésique, ce qui est fondamental pour aligner correctement les contenus AR à l'échelle globale. Au niveau matériel, la standardisation progresse aussi avec OpenXR, interface ouverte gérée par Khronos Group en lien avec l'OGC, visant à

[1135] Maubon Grégory, « Interopérabilité dans le Metaverse : Jérôme Royan nous parle des standards et de la gouvernance », RA'pro, 14 décembre 2021. https://www.augmented-reality.fr/2021/12/interoperabilite-dans-le-metaverse-jerome-royan-nous-parle-des-standards-et-de-la-gouvernance/. Consulté le 8 mai 2024.

[1136] Open Geospatial Consortium, « OGC Augmented Reality Markup Language 2.0 (ARML 2.0) », OGC 12-- 132r4, version 1, 24 février 2015. https://www.ogc.org/standards/arml/. Consulté le 6 janvier 2025.

unifier le développement d'applications XR (RA/RV) sur divers dispositifs [1137]. Enfin, les travaux conjoints du W3C et de l'OGC sur le Web spatial explorent comment le Web 3D et les données géolocalisées peuvent converger, afin que le métavers s'intègre de façon transparente au Web existant [1138].

Malgré ces avancées, des défis importants subsistent pour l'interopérabilité des métavers géographiques. D'une part, la cartographie de référence doit être partagée. Les services de cartographie (fonds de plans 3D, cadastres, modèles de villes) devront être accessibles via des standards ouverts (OGC API, tuiles 3D…) pour servir de toile de fond commune aux expériences immersives. D'autre part, la sémantique des objets virtuels doit être harmonisée : un même bâtiment ou lieu réel doit être identifié de manière univoque à travers différentes plateformes, ce qui renvoie à l'utilisation d'identifiants géographiques normalisés et de dictionnaires communs. Ainsi, il faut considérer les différents niveaux où l'on peut parler d'interopérabilité (matériels, logiciels, data, modèles 3D, interaction, cartographie, etc.), chaque niveau impliquant des standards et gouvernances spécifiques. Par exemple, au niveau des données 3D, l'utilisation conjointe de standards comme CityGML et IFC (Industry Foundation Classes, pour le BIM) est une piste pour assurer qu'un jumeau numérique urbain puisse incorporer à la fois les données géospatiales de la ville et les maquettes détaillées des bâtiments. Au niveau interaction utilisateur, on peut imaginer l'émergence de protocoles communs pour passer d'un espace virtuel à un autre (analogues aux hyperliens du Web, mais en 3D), afin que l'usager naviguant sans rupture entre différentes expériences du métavers.

Les enjeux d'interopérabilité ont également une dimension territoriale et stratégique. Un métavers géographique véritablement interopérable permettrait à une collectivité locale de mélanger des couches d'information issues de divers fournisseurs dans une même expérience cohérente pour l'usager. Cela implique des accords de standardisation et de gouvernance, possiblement sous l'égide d'organisations internationales ou de consortiums publics-privés. À l'inverse, le risque d'une absence d'interopérabilité serait la fragmentation du métavers en vase clos, freinant l'innovation et la participation citoyenne. Ouvrir et normaliser les infrastructures géospatiales du métavers apparaît donc indispensable pour tirer parti des réalités augmentées à venir. Une fois ces défis techniques et normatifs relevés, il convient néanmoins de se pencher sur un autre volet critique que sont les vulnérabilités et menaces inhérentes aux environnements immersifs interconnectés.

[1137] Krhonos Group, « OGC and Khronos Form a Liaison to Improve Interoperability within the Geospatial and 3D Graphics Communities », 10 octobre 2018. https://www.khronos.org/news/press/ogc-and-khronos-form-a-liaison-to-improve-interoperability-within-the-geospatial-and-3d-graphics-communities. Consulté le 23 mars 2024.

[1138] Bird Alan J., « W3C and OGC Augmented Reality Pilot », W3C, 7 décembre 2017. https://www.w3.org/blog/2017/w3c-and-ogc-augmented-reality-pilot-an-exciting-adventure-for-w3c/. Consulté le 15 octobre 2024.

2.3 Cybermenaces liées aux environnements immersifs

L'essor des jumeaux numériques et des métavers géographiques s'accompagne d'une surface d'attaque élargie sur le plan de la cybersécurité. En effet, ces systèmes établissent une liaison intime entre le cyberespace et le monde physique, si bien que toute faille informatique peut potentiellement avoir des répercussions concrètes dans la réalité. Par exemple, un jumeau numérique urbain pilotant des infrastructures critiques comme le réseau électrique, ou le trafic routier sur lequel s'appuie la puissance publique pour prendre des décisions (urbanisme, maintenance prédictive) devient une cible de choix. Une intrusion malveillante pouvant altérer les données du jumeau ou en prendre le contrôle pourrait se traduire par des pannes matérielles, des accidents ou une désorganisation du territoire réel. À titre d'exemple, à l'heure où la SNCF cherche à se doter de son propre jumeau numérique, une attaque contre ce même jumeau qui aboutirait à une manipulation des capteurs de sorte à masquer une avarie imminente pourrait avoir des effets désastreux sur l'exploitation et les usagers [1139]. La manipulation de données est ainsi l'une des menaces majeures : des données falsifiées dans le jumeau peuvent entraîner des décisions erronées aux conséquences potentiellement critiques.

Au-delà de l'intégrité des données, la disponibilité des environnements immersifs est à protéger. Un jumeau numérique ou une plateforme de métavers pourrait faire l'objet d'attaques par déni de service, visant à perturber son fonctionnement. Étant donné que ces systèmes reposent sur un flux continu de données provenant d'innombrables capteurs, les surcharger ou les interrompre peut paralyser l'observation de la situation réelle et la prise de décision. Par ailleurs, le nombre élevé d'objets connectés et de capteurs dans un jumeau territorial constitue un vaste champ d'exposition puisque chaque capteur ou composant peut devenir une porte d'entrée pour un attaquant. Cette multiplicité rend la sécurisation complexe, d'autant plus que la diversité des dispositifs implique des mises à jour inégales et des failles potentielles variées. En somme, les environnements immersifs cumulent les défis classiques de la cybersécurité (contrôle d'accès, sécurisation réseau, surveillance des anomalies) avec des enjeux propres à l'informatique spatiale afin de garantir qu'aucun acteur malveillant ne puisse altérer la représentation du territoire elle-même.

Un autre volet critique concerne la confidentialité et la protection des données personnelles dans ces nouveaux espaces. Les dispositifs de réalité augmentée et virtuelle collectent en continu des informations biométriques, comportementales et de localisation sur les utilisateurs[1140]. Caméras

[1139] INCIBE, « Cybersecurity challenges of digital twins: threats and security measures », 5 septembre 2024. https://www.incibe.es/en/incibe-cert/blog/cybersecurity-challenges-digital-twins-threats-and-security-measures. Consulté le 6 janvier 2025.

[1140] Rafique, W.; Qadir, J., « Internet of everything meets the metaverse: Bridging physical and virtual worlds with blockchain », Comput. Sci. Rev. vol. 54, novembre 2024, 100678. https://www.sciencedirect.com/science/article/pii/S1574013724000625. Consulté le 21 avril 2025.

scannant l'environnement, capteurs de mouvement, suivi du regard ou de la voix, autant de données sensibles qui, si compromises, peuvent servir au profilage illicite, à l'usurpation d'identité ou à la surveillance indue. L'intrusion dans un métavers géographique pourrait révéler des informations précises sur les habitudes de déplacement d'une personne, l'intérieur de son domicile, capté par des lunettes de réalité augmentée, voire ses paramètres de santé dans certains usages en santé immersive[1141]. Une préoccupation majeure est donc d'empêcher les fuites de données depuis ces plateformes. Un stockage chiffré, des politiques strictes sur l'utilisation et la minimisation des données collectées, ainsi que le respect des régulations (RGPD en Europe, etc.) sont indispensables. Par ailleurs, la vérification d'identité dans le métavers pose question. Des cybercriminels pourraient usurper l'apparence virtuelle d'autrui afin de tromper des participants et accéder à des informations ou opérations sensibles. La lutte contre ces deepfakes immersifs nécessitera des mécanismes d'authentification robustes pour chaque acteur virtuel.

Face à ces risques protéiformes, des référentiels de sécurité commencent à émerger pour guider la protection des jumeaux numériques et métavers. Le NIST aux États-Unis a proposé en 2025 un cadre de sécurité dédié aux digital twins, soulignant que *« l'adoption et le respect des standards permettent d'assurer l'interopérabilité, la compatibilité, la sûreté et la cybersécurité* […] *et qu'une implémentation correcte de ces standards inspire crédibilité et confiance »*[1142]. Ce cadre préconise une approche structurée combinant standards d'interopérabilité (protocoles d'échange de données sécurisés), contrôles de cybersécurité (mesures de protection actives contre les menaces) et mécanismes de confiance (authentification et validation des acteurs). De même, les organismes comme l'ANSSI attirent l'attention sur la nécessité d'évaluer les risques tout au long du cycle de vie de ces projets, d'intégrer des solutions de monitoring actif et de cloisonner les différentes composantes du système pour contenir d'éventuelles intrusions.

De plus, il convient d'anticiper les scénarios de menace les plus critiques spécifiques aux environnements immersifs. Par exemple, un jumeau numérique municipal compromis pourrait permettre à un acteur malveillant de prendre en otage des services urbains : un document de sécurité imagine qu'un ex-employé, conservant un accès non révoqué, détourne un jumeau de smart city pour paralyser les transports publics ou la gestion des eaux usées. De tels cas relèvent autant de la cybersécurité opérationnelle que de la cyberdéfense territoriale, et appellent à des plans de réponse aux incidents adaptés. Plus globalement, la protection des métavers géographiques nécessitera d'adopter

---

[1141] Bell, C.; Egon, A.; Broklyn, P., « The Cybersecurity Implication of Extended Reality Technologies: Safeguarding Users in Immersive Environments ». 12 juillet 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4904947. Consulté le 20 décembre 2024.

[1142] Jeffrey Voas (NIST), Peter Mell (NIST), Phillip Laplante (NIST), et Vartan Piroumian, « Security and Trust Considerations for Digital Twin Technology », NIST, IR 8356, février 2025, p. 5. https://csrc.nist.gov/pubs/ir/8356/final. Consulté le 19 mars 2025.

une posture proactive : sécurité by design dans les applications AR/VR, chiffrement systématique des échanges, redondance des capteurs critiques, et collaborations accrues entre experts en SIG et experts en cybersécurité.

En d'autres termes, la sécurisation réussie des jumeaux numériques et métavers géographiques conditionne leur acceptation à long terme. Si les acteurs territoriaux parviennent à instaurer un climat de confiance, où les données spatiales immersives sont fiables, protégées et utilisées de façon éthique, alors ces technologies pourront déployer tout leur potentiel au service des territoires. Ainsi, grâce à des efforts conjoints de normalisation géospatiale, d'interopérabilité et de cybersécurité, l'essor des jumeaux numériques et des métavers géographiques ouvre la voie à une nouvelle ère d'innovations territoriales, tout en rappelant que la confiance dans ces outils devra se construire au même rythme que leur diffusion.

3. Cybersécurité post-quantique et impact sur les standards

Les parties précédentes ont établi les fondations normatives de l'écosystème géospatial émergent, puis examiné leur intégration dans les systèmes les plus avancés de la géomatique contemporaine, les jumeaux numériques territoriaux et métavers géographiques. Ces développements reposent sur un présupposé implicite que la présente partie se propose d'interroger : la robustesse des mécanismes cryptographiques qui garantissent la confidentialité, l'intégrité et l'authenticité des données géospatiales.

L'ensemble de l'architecture normative et technique décrite dans ce chapitre repose sur des primitives cryptographiques dont la sécurité tient à la difficulté computationnelle de certains problèmes mathématiques. La factorisation de grands nombres pour RSA, les logarithmes discrets sur courbes elliptiques pour ECDSA, la résistance aux collisions pour les fonctions de hachage. Cependant, l'émergence de l'informatique quantique menace de rendre ces protections obsolètes. L'algorithme de Shor[1143], exécuté sur un ordinateur quantique suffisamment puissant, permettrait de factoriser en temps polynomial les grands nombres sur lesquels repose RSA[1144], tandis que l'algorithme de Grover réduirait de moitié la sécurité effective des algorithmes symétriques et des fonctions de hachage.

Les implications pour le domaine géospatial sont considérables. Les systèmes d'information géographique, les infrastructures de données territoriales, les services de positionnement par satellite, les registres fonciers sur blockchain, les plateformes d'intelligence artificielle géospatiale, tous ces systèmes analysés dans les parties précédentes reposent sur des fondations cryptographiques que l'informatique quantique menace d'ébranler. Un adversaire disposant de capacités quantiques pourrait intercepter et altérer les flux de données cartographiques, usurper l'identité de serveurs SIG légitimes, falsifier des transactions dans un cadastre blockchain, forger de faux signaux GNSS authentifiés, ou corrompre les données d'entraînement des modèles d'intelligence artificielle géospatiale.

Cette menace systémique appelle une réponse à la hauteur des enjeux. La cryptographie post-quantique, un ensemble d'algorithmes conçus pour résister aux attaques des ordinateurs quantiques tout en restant exécutables sur des machines classiques, constitue la principale ligne de défense. Le

---

[1143] L'algorithme de Shor est un algorithme quantique conçu par le mathématicien américain Peter Shor en 1994. Beaucoup de cryptosystèmes à clé publique, tels que le RSA, deviendraient vulnérables si l'algorithme de Shor était un jour implémenté dans un calculateur quantique pratique. Pour de plus amples informations à ce sujet, lire Shore Peter, « Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer », Proceedings of the 35th Annual Symposium on Foundations of computer Science, Santa Fe, NM, Nov. 20 — 22, 1994. https://arxiv.org/abs/quant-ph/9508027. Consulté le 3 mai 2025.

[1144] Le système de cryptographie RSA (pour Rivest-Shamir-Adleman) est un des systèmes de cryptographie à clé publique les plus utilisés pour la transmission sécurisée de données. Le sigle « RSA » provient des noms de famille de Ron Rivest, Adi Shamir et Leonard Adleman, qui ont décrit publiquement l'algorithme en 1977. Voir à ce sujet, Rivest, R.; Shamir, A.; Adleman, L., « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems », Communications of the ACM, n°21(2), pp. 120 – 126, février 1978. https://dl.acm.org/doi/10.1145/359340.359342

processus de standardisation engagé par le NIST américain, qui a abouti en 2024 à l'adoption des premiers algorithmes post-quantiques (CRYSTALS-Kyber pour l'échange de clés, CRYSTALS-Dilithium pour les signatures numériques), marque une étape décisive. Mais la transition vers ces nouveaux standards représente un défi technique et organisationnel considérable, particulièrement pour les infrastructures géospatiales qui intègrent des systèmes hérités, des protocoles normalisés et des contraintes spécifiques.

Au-delà de sa dimension technique, la transition post-quantique constitue un enjeu géopolitique majeur. La course à l'informatique quantique oppose les grandes puissances dans une compétition où se jouent la suprématie technologique, la capacité de renseignement et l'autonomie stratégique. Le pays qui maîtrisera le premier un ordinateur quantique opérationnel disposera d'un avantage décisif, capable de briser les protections de ses adversaires tout en sécurisant ses propres systèmes. Dans ce contexte, la capacité à définir et à imposer les standards de la cryptographie post-quantique devient un instrument de puissance normative, prolongeant les dynamiques de diplomatie normative analysées dans les parties précédentes.

La présente partie examine ces enjeux selon trois axes. Elle analyse d'abord les vulnérabilités spécifiques des infrastructures géospatiales face aux technologies quantiques : serveurs SIG, bases de données territoriales, systèmes GNSS, registres blockchain, pipelines d'intelligence artificielle. Elle présente ensuite les stratégies de transition vers la cryptographie post-quantique et leur impact sur les standards géospatiaux, en examinant les algorithmes retenus par le NIST, les approches hybrides de migration et les adaptations nécessaires des protocoles OGC et ISO. Elle se conclut en situant ces évolutions dans le contexte géopolitique de la compétition quantique mondiale, analysant les doctrines nationales, les enjeux de souveraineté et les perspectives pour la France et l'Europe.

3.1 Vulnérabilités des infrastructures SIG face aux technologies quantiques

Les progrès de l'informatique quantique font peser de nouvelles menaces cryptographiques sur les systèmes d'information géographique (SIG) et les infrastructures de données territoriales. Les méthodes de cryptographie actuelles, fondées sur la complexité mathématique de problèmes, comme la factorisation ou le logarithme discret, pourraient devenir obsolètes avec l'arrivée d'ordinateurs quantiques suffisamment puissants[1145]. En effet, des algorithmes quantiques tels que celui de Peter Shor permettent de factoriser très rapidement les grands nombres, brisant des schémas à clé publique comme RSA ou les courbes elliptiques, tandis que celui de Grover[1146] permet d'accélérer la recherche dans l'espace des clés symétriques, réduisant de moitié la sécurité effective des algorithmes de chiffrement symétrique et des fonctions de hachage. Autrement dit, un acteur malveillant disposant d'un ordinateur quantique pourrait casser les mécanismes actuels d'authentification et de chiffrement qui protègent les données géospatiales, compromettant la confidentialité, l'intégrité et l'authenticité de ces données critiques. Cette éventualité n'est plus théorique : des experts estiment qu'à l'horizon 2030-2035, de tels ordinateurs quantiques capables de casser RSA-2048 verront probablement le jour [1147]. Par conséquent, la préparation à la menace quantique est désormais considérée comme une priorité de cybersécurité, notamment pour les infrastructures critiques nationales [1148].

Ainsi, parmi les menaces susceptibles de peser sur les infrastructures de systèmes d'information géographique (SIG) à l'ère du calcul quantique, plusieurs vecteurs d'attaque doivent être considérés avec sérieux. L'un des plus redoutés concerne la possibilité, pour un adversaire doté de capacités quantiques, d'intercepter des flux de données géospatiales chiffrées, afin de les stocker en vue d'un déchiffrement ultérieur. Cette stratégie, souvent qualifiée d'attaque « stocker maintenant, déchiffrer plus tard », repose sur la perspective qu'un ordinateur quantique sera un jour en mesure de briser les systèmes cryptographiques classiques et de révéler, a posteriori, des informations sensibles. Un autre scénario redouté repose sur l'exploitation de l'algorithme de Shor, qui permet le rétrocalcul des clés privées à partir de clés publiques. Cette vulnérabilité touche directement les infrastructures

---

[1145] Junquera-Sánchez Javier, Hernando-Ramiro Carlos, Oscar Gamallo-Palomares, Gómez-Sánchez José-Antonio, « Assessment of cryptographie approches for a quantum-résistant Galileo OSNMA », *NAVIGATION : Journal of the Institut of Navigation*, Vol. 71(2), 2024. https://navi.ion.org/content/71/2/navi.648

[1146] L'algorithme de Grover est un algorithme quantique mis au point par le mathématicien indo-américain Lov Kumar Grover en 1996. Il s'agit de l'algorithme quantique de recherche dans une base de données non hiérarchisée le plus efficace jamais mis au point. Pour plus d'informations, consulter Grover Lov, « A fast quantum mechanical algorithm for database search », dans *Proceedings*, 28th Annual ACM Symposium on the Theory of Computing, 1996, p. 212. https://arxiv.org/abs/quant-ph/9605043.

[1147] J. Kearney Joseph et Perez-Delgado Carlos A., « Vulnerability of Blockchain Technologies to Quantum Attacks », *Array*, Vol. 10, juillet 2021. https://www.sciencedirect.com/science/article/pii/S2590005621000138.

[1148] BSI - Fédéral Office for Information Security, « Securing Tomorrow, Today: Transitioning to PostQuantum Cryptography », 27 novembre 2024. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5

d'authentification, telles que les certificats de serveurs cartographiques ou les identifiants d'utilisateurs. En obtenant une clé privée à partir de sa clé publique associée, un acteur malveillant pourrait usurper une identité légitime, falsifier des signatures numériques ou manipuler des certificats d'authentification. Il devient alors possible de générer de faux documents d'urbanisme, de signer frauduleusement des transactions dans une chaîne de blocs, ou encore d'accéder sans autorisation à des plateformes SIG normalement protégées par des mécanismes cryptographiques à clé publique. La sécurité des fonctions de hachage, qui assurent l'intégrité des données géographiques, est également mise à mal par l'ordinateur quantique. L'algorithme de Grover, en particulier, affaiblit significativement la robustesse de ces fonctions. Cela ouvre la voie à la fabrication de données modifiées, telles que des cartes altérées, qui produiraient un hachage identique à celui d'un fichier authentique, rendant ces manipulations indétectables lors des vérifications d'intégrité. De telles attaques compromettent non seulement la fiabilité des bases de données cartographiques, mais aussi celle des engagements cryptographiques sur lesquels reposent certaines chaînes de certification ou d'enregistrement blockchain.

Enfin, il convient de souligner que la menace quantique ne se limite pas aux communications futures. Les données actuellement stockées sous forme chiffrée, bien que protégées par des algorithmes classiques, sont également en péril. Si elles sont interceptées aujourd'hui, elles pourraient être décryptées dans les années à venir lorsque les capacités de calcul quantique auront atteint une maturité suffisante. C'est pourquoi plusieurs agences européennes de cybersécurité mettent en garde contre une exposition prolongée de données sensibles. En novembre 2024, une déclaration conjointe intitulée *Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography*, initiée par la France, l'Allemagne et les Pays-Bas, a été signée par les agences de cybersécurité de dix-huit États membres de l'Union européenne, parmi lesquelles l'ANSSI française, le BSI allemand, le Centre for Cybersecurity Belgium, l'Agenzia per la Cybersicurezza Nazionale italienne ou encore le National Cyber Security Centre néerlandais. Cette déclaration qualifie la transition vers la cryptographie post-quantique de *« priorité absolue »* pour les infrastructures critiques et recommande de protéger les cas d'usage les plus sensibles contre les attaques de type *« stocker maintenant, déchiffrer plus tard »* dès que possible, et au plus tard d'ici fin 2030[1149]. Faute d'une transition rapide vers des solutions de chiffrement post-quantique, des informations considérées aujourd'hui comme confidentielles pourraient être exposées demain, compromettant la souveraineté informationnelle et la sécurité des infrastructures géonumériques.

[1149] BSI - Federal Office for Information Security, « Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography », 27 novembre 2024. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?

Ces menaces plaident pour une remise en question urgente des mécanismes de cybersécurité concernant les données géographiques. Les systèmes d'information géographique et les bases de données spatiales sont au cœur de la gestion territoriale moderne. Ils stockent et échangent des données géoréférencées sensibles, dont la protection repose sur le chiffrement et sur des protocoles d'authentification. Or, l'arrivée de l'informatique quantique menace directement ces mesures de sécurité. Ainsi, les serveurs SIG utilisent souvent TLS avec des certificats RSA ou ECC pour sécuriser les échanges Web de données cartographiques. Un attaquant quantique pourrait casser de tels certificats et intercepter ou altérer les flux de données à l'insu des administrateurs. De même, les bases de données géospatiales chiffrées pourraient être déchiffrées par force brute quantique si elles utilisent des algorithmes vulnérables.

Les conséquences d'une telle brèche cryptographique seraient potentiellement dévastatrices. Un adversaire capable de lire ou modifier à volonté des données géographiques critiques pourrait, par exemple, voler des plans de réseaux stratégiques (gaz, électricité, télécom), révéler des emplacements confidentiels, ou saboter des systèmes d'aide à la décision territoriale en y injectant de fausses données. Un scénario où une puissance étrangère intercepte en temps réel les données d'un SIG gouvernemental français et les corrompt subtilement, via la modification des couches cartographiques relatives à la logistique militaire, ou encore l'effacement de certaines informations topographiques cruciales, afin de perturber la gestion de crise ou la défense du territoire, pourrait tout à fait être envisagé. Sans la résistance aux attaques quantiques, les garanties de confiance dans les données géographiques nationales, pourraient s'effondrer.

De plus, la dimension temporelle aggrave le risque. Ainsi, si une base de données foncières ou environnementales chiffrée aujourd'hui en AES-256[1150] pourrait sembler sûre, en réalité un attaquant opportuniste peut en enregistrer une copie chiffrée et attendre quelques années qu'un ordinateur quantique émerge pour la déchiffrer. Ce délai de vulnérabilité latente, combiné à l'inertie de modernisation des systèmes, place les organismes géographiques dans une course contre la montre. Les agences de cybersécurité recommandent d'ores et déjà de recenser tous les actifs cryptographiques et de planifier la transition vers des algorithmes post-quantiques, sous peine de voir des données stratégiques du territoire exposé.

Enfin, les SIG intègrent de plus en plus de services en ligne et d'architectures distribuées (services Web de cartographie, API de géocodage, etc.), parfois via des standards ouverts incluant des volets de sécurité. La communauté de la géomatique, en collaboration avec les experts en

[1150] Advanced Encryption Standard ou AES est un algorithme de chiffrement symétrique. Le système cryptographique AES est très fréquemment associé à la sécurisation de l'affichage des pages Web ou des échanges de mails à travers l'usage de TLS. Son utilisation est extrêmement répandue. https://luxsci.com/blog/256-bit-aes-encryption-for-ssl-and-tls-maximal-security.html.

cryptographie, devra adapter ces standards de données géospatiales pour y intégrer des solutions de cryptographie post-quantique fiables. En effet, sans cela, l'interopérabilité et la standardisation, censées renforcer la souveraineté numérique en assurant une maîtrise publique des données, pourraient au contraire devenir des voies d'entrée pour des attaques quantiques si les protocoles standards restent fondés sur des algorithmes cassables. Les registres fonciers, cadastres, bases de données d'actes notariés, systèmes d'enregistrement des titres de propriété sont des composantes essentielles de la souveraineté territoriale et de l'économie d'un pays. La numérisation de ces registres, avec parfois l'adoption de technologies blockchain ou de bases de données distribuées pour garantir l'intégrité des transactions foncières, apporte des gains de transparence et de sécurité, tout en introduisant de nouvelles dépendances à la cryptographie. Ainsi, certaines initiatives en Suède, à Dubaï, ou encore au Mali, ont commencé à utiliser la blockchain pour l'enregistrement des terrains et propriétés [1151]. Par design, une blockchain rend la falsification des informations extrêmement difficile tant que les clés cryptographiques restent sécurisées[1152], mais si ces clés sont compromises, l'ensemble du système peut vaciller. L'informatique quantique menace les cadastres numériques de deux façons principales. D'une part, en brisant les schémas d'authentification classiques : un contrat de vente immobilière électronique, signé numériquement par un notaire avec une clé RSA, pourrait être falsifié si un attaquant calcule la clé privée correspondante et génère une signature contrefaite. D'autre part, pour les cadastres basés sur blockchain, la sécurité des portefeuilles, qui contient les clés privées des propriétaires, est un point faible bien connu. Un ordinateur quantique pourrait voler ces clés en cassant l'ECDSA ou RSA qui les protège, permettant de s'approprier des titres fonciers ou d'inscrire de fausses transactions dans le registre. Par exemple, un pirate informatique pourrait calculer la clé privée d'une autorité cadastrale nationale et l'utilise pour réécrire l'historique des transactions foncières. Il pourrait transférer clandestinement des parcelles stratégiques vers des entités fictives, ce qui pourrait avoir de graves conséquences sur le plan juridique et territorial. Ce type d'attaque, bien que complexe, illustrerait une atteinte directe à la souveraineté nationale par le cyberespace quantique, car il éroderait la confiance dans un pilier de l'État de droit.

Il est à noter que la communauté technico-juridique explore déjà des parades, comme l'utilisation de signatures post-quantiques pour les documents officiels, ou l'hybridation des blockchains (intégration de mécanismes de résistance quantique parallèlement aux mécanismes existants). Cependant, ces solutions sont encore naissantes. D'ici à ce qu'elles deviennent des standards

---

[1151] Diarrah Séga, « La Blockchain dans la prévention et la gestion des conflits sociaux en Afrique : cas du foncier au Mali », Livre blanc, juillet 2018. https://d1wqtxts1xzle7.cloudfront.net/56982379/Livre_Blanc-libre.pdf

[1152] Quantumrun, « Blockchain dans l'administration foncière : Vers une gestion foncière transparente », 5 février 2024 https://quantumrun.com/fr/perspicacit%C3%A9/Administration-fonci%C3%A8re-blockchain-vers-une-gestion-transparente-des-terres

opérationnels, les cadastres numériques restent exposés. La France, qui comme la plupart des États occidentaux mise sur la dématérialisation et éventuellement la blockchain pour moderniser ses procédures foncières, devra veiller à anticiper cette transition cryptographique pour ne pas compromettre sa souveraineté territoriale numérique. Cela rejoint les préoccupations de standardisation et de certification abordées précédemment dans le chapitre VIII. La certification des données géographiques par blockchain, si elle est actuellement prometteuse pour garantir l'intégrité des documents d'urbanisme ou des données d'aménagement, perdra toute sa valeur si la blockchain sous-jacente est vulnérable aux ordinateurs quantiques. Ainsi, la résilience post-quantique doit devenir un critère de certification à part entière, intégré aux normes de gestion foncière.

Un autre sujet de préoccupation concerne la protection des systèmes globaux de navigation par satellite, qui aujourd'hui fournissent des services de positionnement et de synchronisation temporelle indispensables aux activités civiles et militaires modernes. Ils sont notamment utilisés pour la navigation terrestre, maritime, aérienne, la gestion du trafic, la synchronisation des réseaux électriques et télécom, etc.,[1153]. La fiabilité des signaux GNSS est donc critique pour les infrastructures territoriales. Au cours des dernières années, des mécanismes d'authentification ont été introduits pour contrer les attaques de brouillage et usurpation (spoofing) qui se multiplient. Par exemple, le service OSNMA de Galileo offre une authentification cryptographique des messages de navigation, unique en son genre dans les GNSS civils [1154].

Cependant, cette sécurité repose elle aussi sur des algorithmes cryptographiques classiques. Or, comme l'ont montré des analyses récentes, Galileo OSNMA n'est pas encore prêt à affronter la menace quantique puisqu'il utilise des courbes elliptiques pour la phase d'initialisation, qui deviendraient vulnérables à une attaque par ordinateur quantique, compromettant l'authenticité des signaux [1155]. Concrètement, si un adversaire disposait d'un calculateur quantique capable de casser l'ECDSA ou autre schéma utilisé dans Galileo, il pourrait calculer les clés secrètes d'OSNMA et ainsi forger de fausses transmissions GNSS qui seraient acceptées comme légitimes par les récepteurs. Cela permettrait des scénarios de spoofing indétectables. Par exemple, un pirate informatique pourrait faire croire simultanément à des milliers de véhicules, drones ou navires que leurs positions sont ailleurs (avec de fausses coordonnées signées « authentiques »), entraînant des perturbations massives, des accidents ou des détournements. Pour les applications militaires ou de sécurité civile, l'impact serait potentiellement catastrophique si les utilisateurs perdent confiance dans le système de positionnement.

[1153] Krenila Michal, « Quantum technology for military applications », EPJ Quantum Technology, 6 november 2021. https://epjqt.epj.org/articles/epjqt/abs/2021/01/40507_2021_Article_113/40507_2021_Article_113.html

[1154] Junquera-Sánchez Javier, Hernando-Ramiro Carlos, Oscar Gamallo-Palomares, Gómez-Sánchez José-Antonio, « Assessment of cryptographie approches for a quantum-résistant Galileo OSNMA », *NAVIGATION : Journal of the Institut of Navigation*, Vol. 71(2), 2024. https://navi.ion.org/content/71/2/navi.648

[1155] Ibid.

Au-delà de Galileo, c'est la protection de l'ensemble des GNSS et système de géolocalisation qui doit être envisagé. Le GPS, par exemple, est intégré dans d'innombrables applications et, bien que son signal civil n'ait pas encore d'authentification cryptographique généralisée, les signaux militaires sont chiffrés. Si ces derniers reposent sur des clés ou certificats vulnérables aux quantiques, un attaquant pourrait décrypter les codes P (Y) ou M du GPS militaire, provoquant un risque d'usurpation d'identité et d'accès au service. De plus, les réseaux terrestres d'appoint comme les balises, ou les systèmes différentiels, utilisent souvent des canaux sécurisés qui seraient également exposés en cas de rupture de la cryptographie.

Face à ces risques, des approches émergent sur le plan technologique. Ainsi, l'utilisation de technologies quantiques elles-mêmes pour sécuriser la navigation, comme les capteurs quantiques inertiels ou l'hybridation quantique-classique pour le Positionnement-Navigation-Temps (PNT). Le Royaume-Uni, par exemple, investit dans un hub de PNT quantique pour disposer de solutions de navigation robustes en environnement dégradé ou en cas de perte du GNSS[1156]. Ces efforts témoignent d'une prise de conscience que la suprématie quantique peut autant servir l'attaque que la défense. Néanmoins, du point de vue de la souveraineté géopolitique, les pays qui maîtriseront les contre-mesures quantiques (PQC pour GNSS, capteurs inertiels avancés) auront un avantage pour garantir la continuité de leurs infrastructures de géolocalisation, tandis que les autres pourraient se retrouver dépendants ou aveugles en cas de perturbation malveillante.

Comme évoqué plus haut, la blockchain est envisagée dans le domaine géospatial pour divers usages allant de la certification de données à la gestion d'actifs territoriaux. L'intérêt réside dans la décentralisation et l'infalsifiabilité des registres distribués, qui peuvent renforcer la confiance sans autorité centrale. Cependant, les blockchains actuelles tirent leur résistance aux fraudes directement de la robustesse de leurs primitives cryptographiques [1157]. Or ces primitives, notamment les algorithmes de signature numérique et les fonctions de hachage, sont précisément celles que l'ordinateur quantique met en danger.

Ainsi, à l'horizon 2035, un ordinateur quantique pourrait casser RSA-2048 ou des courbes elliptiques couramment utilisées. Si une attaque quantique sur un réseau de blockchain liés à des biens géolocalisés se produisait, un attaquant pourrait s'emparer d'actifs numériques associés à la terre ou aux ressources locales si ceux-ci étaient tokenisés ou gérés via blockchain. De même, pour une blockchain privée servant de registre foncier, la compromission d'une seule clé privée de validation

---

[1156] Huntley Robert, « Quantum-Enabled PNT Protects Against GNSS Outages », *EE Times Europe*, 18 novembre 2024. https://www.eetimes.eu/quantum-enabled-pnt-protects-against-gnss-outages/

[1157] Junquera-Sánchez Javier, Hernando-Ramiro Carlos, Oscar Gamallo-Palomares, Gómez-Sánchez José-Antonio, « Assessment of cryptographie approches for a quantum-résistant Galileo OSNMA », *NAVIGATION : Journal of the Institut of Navigation*, Vol. 71(2), 2024. https://navi.ion.org/content/71/2/navi.648

pourrait permettre d'inscrire de fausses transactions et de subvertir l'historique. La blockchain étant par nature un système où la clé fait foi de droit, la perte de contrôle des clés signifie la perte irrémédiable du bien protégé. C'est ce qui rend particulièrement vulnérables les blockchains face aux progrès quantiques.

L'intelligence artificielle appliquée aux données géographiques, si elle ouvre des horizons très prometteurs, n'est pas non plus exempte de nouveaux risques et vulnérabilités. Que ce soit à travers l'usage de réseaux de neurones profonds pour l'analyse d'imagerie satellitaire, de systèmes prédictifs en soutien à l'aménagement urbain, ou encore de modèles d'intelligence artificielle déployés pour la cartographie en temps réel, ces technologies mobilisent des volumes considérables de données géospatiales. Leur fonctionnement repose fréquemment sur une collaboration interinstitutionnelle, impliquant un partage de données entre acteurs publics et privés, parfois à l'échelle transnationale. L'émergence des technologies quantique représente donc un risque pour la chaîne de traitement et de sécurisation de ces systèmes.

Trois vecteurs d'attaque doivent être considérés. Premièrement, l'intégrité des données d'entraînement, pourrait être compromise si les mécanismes cryptographiques qui garantissent leur authenticité devenaient obsolètes, permettant à un adversaire d'introduire des données falsifiées faussant les résultats des algorithmes de planification territoriale. De plus, les modèles de GeoAI eux-mêmes, notamment ceux destinés à la détection d'objets militaires ou à la surveillance environnementale, constituent des actifs critiques dont l'extraction malveillante deviendrait possible en cas de rupture des protocoles de chiffrement. Enfin, les capacités de décryptage quantique pourraient permettre la réidentification d'individus à partir des flux de données supposément anonymisés des villes intelligentes, offrant à une puissance étrangère une cartographie comportementale détaillée de la population d'un territoire. Paradoxalement, l'informatique quantique pourrait aussi renforcer l'IA géospatiale via le quantum machine learning, ce qui renforce l'urgence de sécuriser ces systèmes. La doctrine de cybersécurité post-quantique doit donc s'étendre aux pipelines de données de l'IA, incluant l'inventaire des points de chiffrement et l'adoption de solutions résistantes aux attaques quantiques.

En résumé, l'IA géospatiale, tout en offrant d'immenses possibilités, devient une nouvelle surface d'exposition si ses fondations en matière de données et de modèles ne sont pas protégées contre l'avènement de la quantique. Dans le contexte français, où l'on promeut une IA de confiance, notamment via des initiatives de partage de données territoriales (par exemple, la plateforme GeoAPI ou des data lakes nationaux), il faudra intégrer les algorithmes post-quantiques afin de préserver cette confiance à long terme, et éviter que l'IA ne devienne le maillon faible par lequel la souveraineté numérique du territoire serait compromise.

De plus, la course à l'informatique quantique est devenue un enjeu géopolitique de premier plan, tant pour les opportunités économiques que pour les implications en matière de défense et de renseignement [1158]. Dans cette compétition, quelques pays dominent, les États-Unis et la Chine en tête, investissant massivement dans la R&D quantique et concentrant à eux deux près de 68 % des brevets mondiaux en informatique quantique [1159]. Les États-Unis ont lancé dès 2018 une initiative nationale quantique (National Quantum Initiative Act) dotée d'un budget d'environ 1,2 milliard de dollars sur 5 ans, soutenue par les géants technologiques qui ont déjà atteint des jalons importants, comme démontré par l'annonce de « quantum supremacy » faite par Google en 2019 [1160]. La Chine, de son côté, a fait de la quantique une priorité de son 13e plan quinquennal et investit dans des programmes phares comme le satellite Micius pour communications quantiques en 2016, ou la création d'un laboratoire national quantique à 10 milliards de $, qui lui ont permis de combler son retard en calcul quantique et même de prendre les devants en cryptographie quantique spatiale [1161]. Les grandes puissances voient clairement le double usage de la quantique, celui qui domine cette technologie peut à la fois renforcer ses capacités défensives et offensives.

L'Union européenne a également lancé le programme Quantum Flagship en 2018 avec 1 milliard d'euros sur 10 ans, et la plupart des États membres ont développé des stratégies nationales. Le Royaume-Uni, l'Allemagne, les Pays-Bas ou la France investissent dans des centres de recherche et des startups quantiques prometteuses. La France, par exemple, a annoncé en janvier 2021 un plan quantique national doté de 1,8 milliard d'euros sur 5 ans [1162], visant à faire du pays un leader européen dans ce domaine.

En matière de cybersécurité post-quantique, certains États mettent en place les premières doctrines nationales. Ainsi, les États-Unis ont publié en 2022 le mémorandum de sécurité nationale 10 qui trace une feuille de route pour migrer les systèmes gouvernementaux vers la cryptographie post-quantique, avec des échéances précises et une coordination via le NIST et la CISA [1163]. L'administration américaine exhorte ses agences et les opérateurs d'infrastructures critiques à inventorier les usages cryptographiques et à planifier la transition sans tarder. De même, une déclaration conjointe fin 2024 de 18 agences de sécurité européennes (dont l'ANSSI pour la France) a insisté sur l'urgence de cette

---

[1158] INRIA, « Quels sont les principaux acteurs de l'informatique quantique ? », 16 décembre 2020. https://www.inria.fr/fr/acteurs-informatique-quantique#. Consulté le 12 janvier 2022.

[1159] INPI, « L'informatique quantique dans les brevets en 2024 », novembre 2024, p. 3. https://www.inpi.fr/sites/default/files/INPI_EtudeQuantique_nov.2024_1.pdf#. Consulté le 5 février 2025.

[1160] INRIA, « Quels sont les principaux acteurs de l'informatique quantique ? », 16 décembre 2020. https://www.inria.fr/fr/acteurs-informatique-quantique#. Consulté le 12 janvier 2022.

[1161] Ibid.

[1162] INRIA, « Quels sont les principaux acteurs de l'informatique quantique ? », 16 décembre 2020. https://www.inria.fr/fr/acteurs-informatique-quantique#. Consulté le 12 janvier 2022.

[1163] Cybersecurity & Infrastructure Security Agency, « Post-Quantum Cryptography Initiative », 2021. https://www.cisa.gov/quantum#. Consulté le 8 mai 2023.

transition, la qualifiant de « priorité absolue » pour les infrastructures critiques [1164]. Elles préconisent notamment de déployer des solutions hybrides dès que possible pour parer au risque du « stocker maintenant, déchiffrer plus tard ». Se dessine ainsi un consensus, anticiper le “Q-Day” (date où un ordinateur quantique pourra casser les chiffrements actuels) est crucial pour la sécurité nationale. Certains pays pourraient tenter d’exploiter l’effet de surprise en cachant leurs avancées quantiques le plus longtemps possible afin de prendre de court leurs adversaires. Ainsi, la doctrine chinoise sur le sujet n’est pas publiquement détaillée, alimentant les spéculations sur un écart quantique secret. D’autres prônent la transparence et la coopération internationale (via des instances comme l’OTAN ou l’UIT) pour établir des standards communs de résilience. À ce titre, l’OTAN a publié début 2024 sa première stratégie quantique où elle mentionne explicitement l’objectif de faire passer tous ses systèmes cryptographiques vers des algorithmes quantum-safe[1165], signe que même l’Alliance militaire intègre ce paramètre dans sa posture de défense collective.

Concernant les données géographiques, ces doctrines post-quantiques auront des répercussions directes. Un pays comme la Chine, très en pointe dans les technologies de positionnement et d’observation et parallèlement leader en quantique, pourrait acquérir un ascendant en renseignement géospatial s’il parvient à casser les protections adverses tout en blindant les siennes. De son côté, l’Europe a intérêt à rendre Galileo et ses systèmes de positionnement robustes, sans quoi son ambition d’autonomie serait réduite à néant par une incapacité à contrer des attaques quantiques. En somme, la souveraineté nationale au XXIe siècle comprendra un volet quantique. Les pays en retard risquent de devenir tributaires de ceux qui maîtriseront ces technologies, que ce soit pour obtenir des algorithmes de chiffrement robustes ou pour accéder à des services sécurisés. Au regard des risques émergents posés par le développement de l’informatique quantique, il devient impératif d’initier une transition vers une cybersécurité post-quantique dans le domaine géospatial. Cette mutation technologique doit s’inscrire dans le prolongement des efforts de normalisation et de certification évoqués dans le chapitre VIII, en adoptant une approche systémique, technique et institutionnelle.

Tout d’abord, un des premiers risques concerne l’évolution des fondements cryptographiques des systèmes d’information géographique. La migration vers des algorithmes dits post-quantiques, capables de résister aux capacités de calcul des ordinateurs quantiques, représente un pilier stratégique de cette transformation. De même, les protocoles normalisés par l’OGC pour l’échange de données géographiques devront évoluer pour intégrer des suites cryptographiques post-quantiques, garantissant

[1164] BSI - Fédéral Office for Information Security, « Securing Tomorrow, Today: Transitioning to PostQuantum Cryptography », 27 novembre 2024. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5

[1165] OTAN, « Summary of NATO’s Data Exploitation Framework Policy », 22 octobre 2021. https://www.nato.int/cps/en/natohq/official_texts_210002.htm. Consulté le 16 juillet 2023.

ainsi l'interopérabilité sécurisée dans un futur environnement technologique transformé. Cette transition impose de concevoir des systèmes SIG capables de supporter plusieurs algorithmes cryptographiques simultanément et de s'adapter rapidement à l'évolution des standards et des menaces.

Cependant, la complexité de cette mutation rend nécessaire le recours à des solutions hybrides durant une phase transitoire. Dans cette optique, une combinaison de mécanismes classiques et post-quantiques pour chaque fonction de sécurité critique devra probablement être envisagé. Une telle hybridation, qui permettrait d'assurer la continuité de la sécurité même si l'un des deux mécanismes est compromis, s'illustre notamment par l'utilisation de certificats numériques à double signature ou par un chiffrement en couches successives des bases de données géographiques. Ce type de configuration, par exemple, une signature ECDSA couplée à une signature Dilithium, ou un chiffrement AES doublé d'un algorithme post-quantique, est déjà préconisé par certaines autorités nationales. L'ANSSI, notamment, a publié des recommandations allant dans ce sens, jugeant cette approche comme étant le prix à payer pour conserver un niveau de sécurité satisfaisant pendant la période de transition[1166]. Sa mise en œuvre implique toutefois une modernisation technique étendue, les logiciels SIG devront être mis à jour, les micrologiciels des récepteurs GNSS ajustés, et les contrats intelligents intégrant des composants cryptographiques devront être adaptés. Ces transformations nécessiteront des phases de tests rigoureuses, accompagnées de procédures de certification menées par des entités spécialisées, telles que l'ANSSI ou leurs équivalents européens, afin de vérifier que les performances et la précision géospatiale ne sont pas altérées.

Cette transition technologique doit également s'accompagner d'un renforcement des capacités humaines et institutionnelles. La sécurité post-quantique ne saurait reposer uniquement sur des avancées techniques, elle nécessite aussi une évolution des compétences professionnelles et des modes de gouvernance. Les experts en géomatique devront être formés aux enjeux spécifiques de la post-quantique afin d'intégrer les exigences de sécurité dès la phase de conception des systèmes, dans une logique de « security by design ». Parallèlement, les organismes de normalisation du domaine géospatial, comme l'ISO/TC 211 ou l'OGC, devraient initier une collaboration étroite avec les structures en charge de la standardisation en cryptographie, telles que l'ISO/IEC JTC 1 SC 27 ou l'IETF. Cette collaboration pourrait déboucher sur l'élaboration de lignes directrices transversales, comme un guide de meilleures pratiques post-quantiques pour les infrastructures de données spatiales. Les organismes responsables de la certification des données géographiques devront aussi adapter leurs référentiels, en exigeant des mécanismes de sécurité résistants aux quantiques pour qu'un jeu de

[1166] ANSSI, « Cryptographie post-quantique (PQC) Posture générale et actions de l'ANSSI sur la PQC », octobre 2025. Cryptographie post-quantique (PQC) — ANSSI.

données puisse être authentifié. Il serait même envisageable de compléter les certifications existantes, comme l'ISO/IEC 27001 par un amendement spécifique consacré à la résilience post-quantique.

Ainsi, dans un contexte de menace globale, l'action internationale apparaît comme une voie incontournable. L'Europe dispose aujourd'hui d'atouts indéniables dans le domaine de la cybersécurité quantique, notamment grâce aux programmes collaboratifs financés par Horizon Europe ou aux initiatives de l'ENISA et de l'ESA en matière de sécurisation du spatial. Ces ressources pourraient être mobilisées pour lancer des projets pilotes spécifiquement orientés vers le secteur géospatial. Un démonstrateur de cadastre post-quantique réunissant plusieurs pays, ou une expérimentation conjointe entre l'ESA et EUROCONTROL sur un canal Galileo sécurisé constitueraient des signaux politiques forts et des laboratoires d'innovation collective. Ces expérimentations permettraient d'identifier en amont les obstacles opérationnels et d'orienter les choix stratégiques avant un déploiement à grande échelle. De surcroît, ces dynamiques coopératives contribueraient à rééquilibrer le rapport de force technologique avec les États-Unis ou la Chine, en mutualisant les ressources et en affirmant une souveraineté numérique européenne.

En conclusion, la menace quantique sur les infrastructures géographiques est un enjeu multidimensionnel qui lie intimement cybersécurité, technologies quantiques et souveraineté nationale. La standardisation des données géospatiales et des protocoles doit désormais intégrer ce paramètre quantique pour rester pertinente. La France, à travers ses organismes nationaux et ses partenaires européens, a un rôle clé à jouer pour orienter les normes et les déploiements vers des solutions de confiance post-quantique. Il en va de la protection du cyberespace territorial français face aux puissances qui, demain, disposeront de calculateurs aux capacités sans précédent. À l'aune de cette transition, investir dans la recherche, la normalisation et la sensibilisation autour de la sécurité quantique des SIG et données géographiques apparaît non seulement comme une nécessité technique, mais comme un impératif de souveraineté pour que le domaine géospatial reste un atout et non une faiblesse dans la stratégie nationale.

3.2. Premiers efforts de normalisation pour la protection post-quantique

La menace que font peser les futurs ordinateurs quantiques sur les algorithmes cryptographiques actuels a déclenché, dès la fin des années 2010, une mobilisation mondiale pour développer et standardiser des algorithmes post-quantiques. La cryptographie post-quantique, également désignée sous le terme de cryptographie résistante aux attaques quantiques (quantum-resistant cryptography), se définit, selon le National Institute of Standards and Technology (NIST), comme *« un domaine de la cryptographie qui recherche et développe l'usage de primitives résistantes aux attaques quantiques, avec pour objectif de préserver les infrastructures à clé publique existantes dans une ère future d'informatique quantique »*[1167]. Plus précisément, son objectif est de *« développer des systèmes cryptographiques qui soient sécurisés à la fois contre les ordinateurs quantiques et classiques, tout en restant interopérables avec les protocoles de communication et les réseaux existants »*[1168]. Contrairement à la cryptographie quantique, qui repose sur les propriétés de la physique quantique pour sécuriser les échanges, la cryptographie post-quantique s'appuie sur des problèmes mathématiques réputés difficiles tant pour les ordinateurs classiques que quantiques. À l'horizon 2030–2035 évoqué par les experts pour l'émergence d'ordinateurs quantiques cryptographiquement pertinents, les efforts de normalisation dans ce domaine devront avoir abouti. L'objectif étant de disposer à temps de nouvelles primitives cryptographiques résistantes aux attaques quantiques, afin de protéger durablement les communications numériques, y compris dans le domaine des données géographiques, et de préserver la souveraineté numérique des États.

Plusieurs organismes de standardisation ont lancé des programmes pour évaluer et normaliser de nouveaux algorithmes résistants aux attaques quantiques. Le plus important est le NIST aux États-Unis, qui a initié dès 2016 un vaste processus ouvert de sélection d'algorithmes post-quantiques. Après trois tours d'évaluation impliquant des chercheurs du monde entier, le NIST a annoncé en 2022 un premier ensemble de quatre algorithmes post-quantiques retenus pour la standardisation [1169] : le schéma de chiffrement à base de réseaux CRYSTALS-Kyber[1170] pour l'établissement de clés, et trois schémas de signature numérique (CRYSTALS-Dilithium, FALCON et SPHINCS+)[1171]. Ces choix ont été guidés par des critères de sécurité, de performances, ainsi que par le besoin d'une diversité des bases

---

[1167] NIST, « Post-Quantum Cryptography », https://www.nist.gov/programs-projects/post-quantum-cryptography; voir également NIST Internal Report 8105, Report on Post-Quantum Cryptography, avril 2016, p. 1.

[1168] Ibid

[1169] NIST, « Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process », NIST IR 8413, juillet 2022. https://csrc.nist.gov/pubs/ir/8413/upd1/final. Consulté le 3 janvier 2025.

[1170] CRYSTALS Cryptographic Suite for Algebraic Lattices. https://pq-crystals.org/kyber/index.shtml

[1171] ANSSI, « ANSSI views on the Post-Quantum Cryptography transition », 21 décembre 2023. https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf. Consulté le 20 mars 2023.

mathématiques pour parer à toute faiblesse future. En 2023-2024, le NIST a poursuivi un quatrième tour pour évaluer des candidats supplémentaires, notamment des alternatives fondées sur d'autres problèmes difficiles. Ce processus a abouti en 2025 à la sélection de HQC (Hamming Quasi-Cyclic), un schéma de chiffrement à base de codes, comme algorithme supplémentaire de chiffrement post-quantique[1172]. HQC servira de renfort aux côtés du schéma principal Kyber, basé, lui, sur les réseaux euclidiens modulaires, afin de garantir un standard de rechange en cas de vulnérabilité découverte dans la première option. Parallèlement, les autorités américaines ont commencé à préparer la migration de leurs systèmes vers ces nouveaux algorithmes. La NSA a actualisé dès 2022 sa suite d'algorithmes recommandés en y incluant les premiers algorithmes post-quantiques du NIST (Kyber et Dilithium) pour une adoption d'ici 2030 dans les systèmes classifiés, et la Maison-Blanche a émis des directives fixant l'objectif d'atténuer d'ici 2035 le risque quantique pour l'administration fédérale [1173].

Si ce processus de normalisation cryptographique peut sembler, à première vue, éloigné des préoccupations géographiques, il s'inscrit en réalité au cœur des enjeux de souveraineté territoriale et de géopolitique des données qui structurent cette thèse. D'une part, les infrastructures géospatiales, systèmes d'information géographique, services de positionnement par satellite (GPS, Galileo, BeiDou), cadastres numériques, jumeaux numériques territoriaux, constituent précisément les systèmes critiques que ces nouveaux algorithmes ont vocation à protéger. La sécurité des données de localisation, des cartographies d'infrastructures sensibles et des bases foncières nationales dépend directement de la robustesse des primitives cryptographiques qui les chiffrent et les authentifient. D'autre part, le processus de standardisation lui-même revêt une dimension géopolitique majeure. En effet, le pays ou le bloc qui impose ses standards cryptographiques définit les conditions d'accès, d'échange et de protection de l'information numérique à l'échelle mondiale. En pilotant ce processus, les États-Unis, via le NIST, consolident leur position de prescripteur normatif dans un domaine stratégique, tandis que l'Europe et la Chine s'efforcent de développer des capacités autonomes pour ne pas dépendre d'algorithmes dont ils ne maîtriseraient pas l'évaluation ou l'implémentation. Cette compétition normative prolonge, dans le domaine cryptographique, les dynamiques de diplomatie normative analysées dans les chapitres précédents, la maîtrise des standards de sécurité des données géospatiales conditionne la capacité d'un État à protéger son territoire numérique et à préserver sa souveraineté informationnelle face aux puissances concurrentes.

[1172] NIST, « Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process », NIST IR 8545, mars 2025. https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf. Consulté le 18 mai 2025.

[1173] Moody Dustin, « NIST POST-QUANTUM CRYPTOGRAPHY UPDATÉ », National Institute of Standards and Technbology. Mars 2025. https://csrc.nist.gov/csrc/media/Presentations/2023/nist-post-quantum-cryptography-update/2a-Moody_NIST_PQC_2.pdf#. Consulté le 10 mars 2025.

D'autres organismes internationaux de standardisation collaborent étroitement avec le NIST et contribuent à cette dynamique. L'ISO/IEC (JTC 1 SC 27 sécurités de l'information) travaille à l'intégration des algorithmes post-quantiques dans ses normes. Un amendement à la norme ISO/IEC 18033-2 relative aux schémas de chiffrement asymétrique, est en cours d'élaboration pour y inclure des algorithmes PQC[1174]. De même, l'ISO a développé la norme ISO/IEC 14888-4 : 2024[1175] portant sur les signatures numériques à base de fonctions de hachage, ces schémas de signature dits « avec état » étant résistants aux attaques quantiques par construction. À terme, l'ISO pourrait adopter également les algorithmes sélectionnés par le NIST pour les signatures et le chiffrement post-quantiques, une fois ceux-ci finalisés, assurant ainsi une harmonisation des standards internationaux. Il est notable que, dans les discussions à l'ISO, la communauté ait manifesté le souhait de diversifier les choix par rapport au NIST, par exemple en considérant des variantes plus conservatrices (comme FrodoKEM ou McEliece) en complément de Kyber, afin de lever d'éventuelles suspicions de backdoor ou dépendances excessives envers un seul pays [1176]. Ceci souligne bien l'importance stratégique que revêt la standardisation post-quantique sur la scène internationale, où chaque grand acteur cherche à la fois la sécurité technique et l'autonomie politique.

En Europe, l'ETSI a été un pionnier sur la question de la cryptographie post-quantique. Son comité technique CYBER a mis en place dès 2015 un groupe de travail QSC (Quantum-Safe Cryptography) pour étudier et anticiper les besoins en normalisation. L'ETSI a publié plusieurs rapports techniques de référence synthétisant l'état de l'art et les bonnes pratiques en matière de crypto post-quantique. Plus récemment, l'ETSI est passé à la phase de standardisation active. Ainsi, en mars 2025, l'ETSI a annoncé la publication de sa première spécification de standard post-quantique. Celle-ci porte sur un schéma innovant de clé hybride avec contrôle d'accès, appelé KEMAC/ « Covercrypt », qui combine un chiffrement classique et post-quantique tout en restreignant l'accès aux clés de session via des politiques d'attributs [1177]. Ce standard, l'ETSI TS 104 015, vise à protéger les données sensibles en assurant qu'elles ne pourront être déchiffrées que par des utilisateurs autorisés disposant des attributs requis, et ce, même face à un attaquant équipé d'un ordinateur quantique. L'ETSI prévoit

---

[1174] ISO/IEC 18033-2 : 2006 Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement. Partie 2: Chiffres asymétriques. https://www.iso.org/fr/standard/37971.html

[1175] ISO/IEC 14888-4 : 2024 Sécurités de l'information — Signatures numériques avec appendice. Partie 4: Mécanismes basés sur le hachage à état. https://www.iso.org/fr/standard/80492.html

[1176] Mitchell Chris, « Out with the old: The cryptographic revolution caused by the threat of quantum computing », Computing conference 2024, 2024. https://chrismitchell.net/Talks/240711.pdf. Consulté le 20 décembre 2024.

[1177] ETSI, « ETSI launches new standard for Quantum-Safe Hybrid Key Exchanges to secure future post-quantum encryption », Sophia Antipolis, France, 25 mars 2025. https://www.etsi.org/newsroom/press-releases/2513-etsi-launches-new-standard-for-quantum-safe-hybrid-key-exchanges-to-secure-future-post-quantum-encryption#. Consulté le 10 mai 2025.

d'autres spécifications à venir, par exemple dans le domaine des VPN quantum-safe[1178] ou des architectures de gestion de clés. Ces initiatives complètent le travail du NIST en offrant des implémentations de référence et des schémas complémentaires, et témoignent de la volonté européenne de contribuer concrètement à la panoplie de standards post-quantiques.

La cryptographie post-quantique est donc désormais en voie de standardisation, et se pose de plus en plus la question de son intégration dans les différents secteurs d'application, et en particulier le secteur géospatial. Les infrastructures de données géographiques, les systèmes d'information géographique et les services cartographiques en ligne reposent sur de nombreux standards. Historiquement, ces standards se sont surtout concentrés sur l'interopérabilité sémantique et technique des données, tandis que la sécurité des échanges était prise en charge par des protocoles génériques sous-jacents, comme TLS/HTTPS pour sécuriser les services OGC Web Map Service ou Web Feature Service. Cependant, avec l'arrivée des menaces quantiques, assurer la sécurité des flux géospatiaux devient un enjeu critique, en particulier pour les infrastructures géospatiales sensibles comme les données cadastrales, les cartographies militaires, les systèmes de navigation, ou encore les données d'observation de la Terre. Il est donc nécessaire que la normalisation géospatiale intègre à son tour ces nouvelles normes cryptographiques.

Concrètement, plusieurs niveaux d'intégration sont envisagés. Tout d'abord, les protocoles de communication utilisés dans le domaine géospatial devront adopter des suites cryptographiques post-quantiques une fois celles-ci disponibles. Par exemple, les services Web INSPIRE devront, à l'horizon 2030, exiger l'usage de versions de TLS intégrant des algorithmes d'échange de clés post-quantiques, de façon à garantir la confidentialité à long terme des données échangées [1179]. De même, les API cartographiques grand public évolueront pour utiliser les bibliothèques cryptographiques post-quantiques fournies par les systèmes d'exploitation ou navigateurs, transparence pour l'utilisateur final, mais impératif de compatibilité pour l'éditeur. Les organismes de standardisation Web et géospatiaux devront collaborer pour s'assurer que ces transitions se fassent de façon fluide. L'OGC, via son Groupe de travail sur la Sécurité et en lien avec l'IETF, devra mettre à jour ses bonnes pratiques de sécurisation des services afin de recommander l'utilisation d'algorithmes post-quantiques dès que ceux-ci seront standardisés et implémentés. Des Guides techniques OGC/ISO listant les suites cryptographique quantum-safe à employer pour tel type de service (WMS, WFS, API REST OGC) afin de garantir l'interopérabilité sécurisée pourraient à terme voir le jour.

[1178] Boyer Claire, « ETSI TC Cyber releases Report on Quantum-Safe Virtual Private Networks », Sophia Antipolis, France, 16 octobre 2018. https://www.etsi.org/committee?id=1382 Consulté le 10 mai 2025.

[1179] ENISA, « Post-Quantum Cryptography: Current state and quantum mitigation », 3 mai 2021. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation. Consulté le 22 octobre 2024 ; USGIF, « Is Quantum Computing Poised to Transform GEOINT? », 11 avril 2024. https://usgif.org/is-quantum-computing-poised-to-transform-geoint/ Consulté le 22 octobre 2024.

De plus, il y a l'intégration au niveau des formats de données et métadonnées géospatiales. Actuellement, la protection de l'intégrité et l'authenticité des données géographiques sont rarement prévues dans les standards de données eux-mêmes, il faut généralement s'en remettre à des mécanismes extérieurs (signatures de documents, certificats, etc.). Or, avec la montée des usages critiques, il devient pertinent d'envisager des mécanismes de signature numérique des données géospatiales intégrés aux flux ou aux formats. Par exemple, le standard GeoJSON ou le futur OGC API pourraient spécifier une façon d'inclure une signature post-quantique des entités géographiques transmises, garantissant qu'une couche d'information n'a pas été altérée en transit. De même, les métadonnées INSPIRE décrivant un jeu de données pourraient comporter des champs de certification signés numériquement par l'autorité émettrice, assurant la traçabilité et l'authenticité de la donnée. Pour que de tels mécanismes voient le jour, il faudra que les algorithmes de signature post-quantique soient suffisamment matures et standardisés et que les organisations de normalisation les adoptent comme normes recommandées.

La normalisation de la cryptographie post-quantique constitue donc un enjeu stratégique mondial, chaque grande puissance élaborant sa propre feuille de route pour garantir sa souveraineté numérique face aux menaces induites par l'informatique quantique. En tête de cette dynamique, les États-Unis dominent la scène avec le processus du NIST, adossé à une stratégie nationale pilotée par la Maison-Blanche et la NSA, fixant un objectif de transition complète d'ici 2035[1180]. Cette stratégie est fondée sur une mobilisation étroite entre acteurs publics et privés, visant à faire des standards américains la référence mondiale en matière de PQC. L'Union européenne, coordonne quant à elle activement la transition via l'ENISA et l'ETSI, tout en finançant des projets de R&D, avec une recommandation de la Commission de 2024 appelant à une feuille de route européenne synchronisée[1181]. Ce positionnement met en avant l'objectif d'une migration homogène sur tout le continent, tout en assurant une certaine autonomie stratégique vis-à-vis des grandes puissances extraeuropéennes. Au sein de l'UE, la France se distingue par son activisme normatif et industriel. Via l'ANSSI, elle adopte une approche hybride prudente et proactive, soutenue par des investissements publics et vise la délivrance de certifications post-quantiques dès 2024[1182]. La stratégie française

---

[1180] Young Shalanda D., « Enhancing the Security of the Software Supply Chain through Secure Software Development Practices », Executive Office of The President Office of Management and Budget, M-22-18, 14 septembre 2024. https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf. Consulté le 30 novembre 2024.

[1181] Commission Européenne, « RECOMMANDATION de la Commission du 11.4.2024 relative à une feuille de route pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique », Bruxelles, le 11 mars 2024, C(2024) 2393 final. https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography. Consulté le 22 mai 2024.

[1182] ANSSI, « ANSSI views on the Post-Quantum Cryptography transition », 21 décembre 2023. https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf. Consulté le 20 mars 2023.

articule ainsi rigueur cryptographique, calendrier industriel et affirmation de la souveraineté nationale dans un cadre européen. La Chine quant à elle poursuit une stratégie plus autonome. Dès 2018, elle a lancé son propre concours national, sélectionnant en 2020 des algorithmes proches de Kyber et Dilithium (Aigis), illustrant sa volonté de contrôler ses propres standards tout en s'appuyant sur l'expertise internationale disponible [1183]. Beijing vise ainsi à sécuriser ses infrastructures critiques avec des normes domestiques, tout en se préparant à imposer ses choix dans les instances normatives internationales. En parallèle, la Russie s'inscrit dans un tempo plus discret et lent. Les travaux du comité TC26 ont généré quelques propositions comme SHIPOVNIK ou FORZITSIYA, mais le processus reste opaque et a subi un revers avec l'invalidation de SIKE, un algorithme inspirant certaines de ses variantes [1184]. Malgré cette prudence, la Russie semble déterminée à ne pas dépendre de standards occidentaux, bien qu'elle accuse actuellement un retard notable. L'Inde amorce également une structuration stratégique autour de la cryptographie post-quantique. Bien qu'elle ne possède pas encore de standards nationaux établis, elle manifeste un intérêt croissant pour l'adoption des algorithmes du NIST [1185]. L'Inde semble donc prête à s'aligner sur les standards internationaux tout en affirmant sa souveraineté numérique émergente. Enfin, le Japon, fidèle à sa tradition technologique et coopérative, s'aligne aussi sur les choix du NIST. Par l'intermédiaire du comité CRYPTREC, il prévoit d'intégrer les standards américains dans sa politique publique, tout en soutenant une forte activité de R&D nationale et des expérimentations industrielles sur le terrain. Sa stratégie repose sur un modèle pragmatique d'intégration rapide, de contribution scientifique et de déploiement concret.

En dehors des acteurs majeurs ci-dessus, d'autres nations ou régions ont également initié des efforts, souvent en lien avec leurs alliances. Le Royaume-Uni, par exemple, via le NCSC, participe à l'élaboration de standards post-quantiques aux côtés des États-Unis et de l'ETSI, et oriente ses recommandations vers l'adoption des algorithmes NIST dès que possible. Le Canada, l'Australie et la Nouvelle-Zélande, autres membres des Five Eyes, ont des approches similaires alignées sur celle des USA/NIST. L'Allemagne, via le BSI, a été l'une des premières en Europe à publier des lignes directrices sur la migration post-quantique, insistant comme la France sur l'usage de solutions hybrides et la planification anticipée [1186]. La Corée du Sud a la particularité d'avoir déjà standardisé quatre

---

[1183] Barshteyn, « A Brief Survey of World Post-Quantum Cryptography Standardization Efforts », 2022.

[1184] National Technical Committee 260 on Cybersecurity of the Standardization Administration of China, « Guide des pratiques standard en matière de cybersécurité (网络安全标准实践指南) », août 2022. https://www.tc260.org.cn/front/cbw.html?start=0&length=4&type=3. Consulté le 5 septembre 2024.

[1185] Prateek Tripathi, « Post-Quantum Cryptography: The lynchpin of future cybersecurity », Observer Research Foundation, 4 décembre 2023. https://www.orfonline.org/expert-speak/post-quantum-cryptography-the-lynchpin-of-future-cybersecurity. Consulté le 23 février 2024.

[1186] BSI, « Technical guideline on cryptographic mechanisms: Recommendations and key lengths », 2023. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile. Consulté le 6 janvier 2024.

algorithmes post-quantiques nationaux pour certains usages locaux, tout en prévoyant de supporter également les standards internationaux une fois finalisés[1187]. Enfin, des pays comme l'Ukraine ont surpris en standardisant dès 2019 un algorithme post-quantique national nommé DSTU 8961 « SKELYA » [1188], montrant que même des pays hors du cercle des grandes puissances prennent la mesure de ces enjeux pour la sécurité de leurs communications souveraines. Toutes ces initiatives nationales dessinent un espace mondial où la coopération internationale reste forte, mais où chacun souhaite garantir ses intérêts.

L'essor de la cryptographie post-quantique ne constitue pas qu'une simple évolution technique, il soulève aussi des enjeux stratégiques liés à la souveraineté numérique et à la sécurité des infrastructures critiques, notamment territoriales. Dans le contexte français et européen, la standardisation post-quantique se conçoit conjointement avec la volonté de garantir l'autonomie stratégique en cybersécurité. Comme évoqué plus haut, disposer de normes et d'implémentations maîtrisées permet de ne pas dépendre exclusivement de puissances étrangères pour la sécurité des données nationales. Par exemple, le fait que l'ISO envisage d'inclure dans ses standards non seulement les algorithmes NIST (Kyber), mais aussi des alternatives comme Frodo ou McEliece répond en partie à ce besoin de souveraineté technique, en assurant qu'en cas de doute sur un algorithme dominé par un pays, on puisse se replier sur un autre [1189]. De même, l'accent mis en France sur la certification de produits intégrant de la post-quantique vise à développer un écosystème local de confiance apte à équiper les administrations et opérateurs nationaux sans recourir systématiquement à des solutions importées.

Ainsi, au-delà des mesures techniques et des calendriers de migration, la normalisation de la cryptographie post-quantique révèle donc des rapports de force géopolitiques structurants qui engagent la hiérarchie mondiale de la puissance numérique.

En premier lieu il y a celui de l'hégémonie normative. En pilotant le processus de standardisation le plus avancé et le plus ouvert, les États-Unis s'assurent que leurs algorithmes, notamment CRYSTALS-Kyber et CRYSTALS-Dilithium, deviennent la référence mondiale, contraignant de facto l'ensemble des acteurs internationaux à adopter des primitives cryptographiques conçues, évaluées et validées sous supervision américaine. Cette position de prescripteur normatif confère aux États-Unis un avantage stratégique considérable via la maîtrise des spécifications

---

[1187] KISA, « Quantum-résistant cryptographie », 2025. https://seed-kisa-or-kr.translate.goog/kisa/ngc/pqc.do?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp. Consulté le 30 avril 2025.

[1188] Yurii I. Gorbenko, Kateryna O. Kuznetsova, Ivan D. Gorbenko, Alexandr A. Kuznetsov, « Featured Article: post-quantum cryptographie: the first results of standardization », NCT, juin 2022. https://ctsoc.ieee.org/images/CTSOC-NCT-2022-06-FA.pdf. Consulté le 2 avril 2025.

[1189] Mitchell Chris, « Out with the old: The cryptographic revolution caused by the threat of quantum computing », Computing conference 2024, p. 15, 2024. https://chrismitchell.net/Talks/240711.pdf. Consulté le 20 décembre 2024.

techniques, l’influence sur les implémentations logicielles, et la capacité potentielle à identifier des faiblesses avant les autres.

Il y a également celui de l'autonomie stratégique. La Chine, en développant ses propres algorithmes via un concours national parallèle, refuse explicitement de dépendre de standards occidentaux pour la protection de ses infrastructures critiques, qu'il s'agisse des réseaux de télécommunications, du système BeiDou ou des bases de données gouvernementales. Cette stratégie de découplage normatif s'inscrit dans la doctrine plus large de « souveraineté cybernétique » analysée dans les chapitres précédents, Beijing souhaite contrôler l'intégralité de la chaîne de confiance numérique, du matériel aux algorithmes, pour se prémunir contre toute dépendance ou vulnérabilité imposée de l'extérieur.

De plus, il faut également signaler celui de la fragmentation normative. La coexistence de standards américains, chinois et potentiellement russes fait peser le risque d'un « splinternet cryptographique » où les systèmes d'information des différents blocs deviendraient incompatibles, entravant les échanges de données et créant des zones d'interopérabilité fermées. Pour les infrastructures géospatiales, qui reposent sur des flux de données transnationaux, tels que l'imagerie satellitaire, les services GNSS ou la cartographie collaborative, cette fragmentation constituerait un obstacle majeur à la coopération internationale.

Enfin, il y a celui de la dépendance pour les puissances moyennes et émergentes. L'Inde, le Japon et la plupart des pays européens n'ont pour l’instant pas les capacités de développer et d'évaluer leurs propres algorithmes post-quantiques, ces derniers devront nécessairement adopter des standards étrangers, américains ou chinois, pour sécuriser leurs infrastructures. Ce choix d'alignement normatif engage leur souveraineté numérique à long terme. En effet, adopter les standards du NIST, c'est accepter une forme de dépendance technologique vis-à-vis de Washington, tandis qu’adopter les standards chinois, c'est s'inscrire dans l'orbite numérique de Beijing. L'Union européenne tente de naviguer entre ces écueils en coordonnant une transition commune via la recommandation de la Commission de 2024 et en finançant une recherche et développement autonome, mais elle reste structurellement dépendante des algorithmes américains pour ses déploiements à court terme. Enfin, le cinquième enjeu est celui de l'asymétrie temporelle. Le pays qui maîtrisera le premier un ordinateur quantique cryptographiquement pertinent, avant que ses adversaires n'aient achevé leur migration post-quantique, disposera d'une fenêtre d'opportunité stratégique pour déchiffrer les communications interceptées, compromettre les infrastructures critiques et obtenir un avantage informationnel décisif. La course à la normalisation post-quantique est donc indissociable de la course à l'informatique quantique elle-même, les deux compétitions se renforcent mutuellement et dessinent les contours d'un nouvel équilibre des puissances dans le cyberespace.

En conclusion, les premiers efforts de normalisation pour la protection post-quantique montrent une mobilisation générale, à la hauteur du défi que représente l'ordinateur quantique pour la sécurité du cyberespace. Du concours NIST aux recommandations de l'ENISA, en passant par les plans d'action nationaux, une multitude d'acteurs œuvrent de concert pour que, lorsque le jour viendra, les données géographiques, les infrastructures territoriales et les systèmes numériques certifiés demeurent sûrs et souverains. Ce mouvement de fond en cryptographie s'articule intimement avec les autres pans de la révolution géonumérique, en fournissant le socle de confiance sans lequel aucune souveraineté numérique ne peut être assurée. La France et l'Europe, en particulier, se doivent de jouer un rôle moteur dans cette transition, pour que la protection du cyberespace géospatial de demain reflète leurs valeurs, garantisse leur autonomie et protège leurs citoyens. Les chapitres suivants approfondiront ces synergies en examinant comment l'IA géospatiale et la blockchain peuvent bénéficier de ces nouveaux standards de sécurité, et comment l'ensemble concourt à renforcer la résilience et la confiance dans les systèmes d'information géographiques à l'ère de la quantique.

3.3 coopération internationale pour la sécurité quantique des données géographiques

Face au risque qu'un ordinateur quantique puisse briser les chiffrements actuels, et malgré l'intensification de la compétition internationale en matière de développement des technologies quantiques, les États multiplient les collaborations pour sécuriser les données, y compris géospatiales, dans l'anticipation de l'émergence d'un monde post-quantique. Des accords bilatéraux émergent, par exemple entre l'Union européenne et les États-Unis via le Trade and Technology Council, qui intègre des discussions sur la cryptographie post-quantique. De même, le partenariat AUKUS (Australie–Royaume-Uni–USA) inclut la coopération sur les technologies quantiques militaires, traduisant une volonté d'alignement stratégique entre alliés. Parallèlement, des cadres multilatéraux comme l'OTAN et le QUAD (Dialogue quadrilatéral sur la Sécurité regroupant États-Unis, Japon, Inde, Australie) ont fait de la résilience quantique une priorité partagée depuis 2023. Une analyse récente recommande d'ailleurs au QUAD de coordonner le développement de standards cryptographiques post-quantiques via un réseau de coopération en normalisation [1190], et de renforcer les capacités de protection des données critiques face à la menace quantique. Ces efforts témoignent d'une compréhension commune que la transition vers des systèmes de chiffrement quantum-safe nécessitera une réponse collaborative à l'échelle internationale [1191]. En effet, les États occidentaux traditionnellement alliés considèrent que le défi quantique exige des « partenariats » et une « standardisation » coordonnée entre gouvernements pour définir les réponses appropriées [1192].

Plusieurs enceintes internationales intègrent la sécurité post-quantique dans leurs travaux, avec un accent particulier sur les données sensibles, comme l'information géographique. L'ONU sert de forum de dialogue général sur la cybersécurité, mais c'est surtout au sein de l'UIT que se concrétisent des efforts en matière de normalisation des technologies quantique. Par exemple, l'UIT-T a développé une série de recommandations Y.3800 pour encadrer les réseaux de distribution quantiques de clés (QKD)[1193], réunissant des experts du monde entier dans une démarche de standardisation globale. L'OTAN, de son côté, a identifié les technologies quantiques comme un « game changer » pour la

---

[1190] Australian Government, «2023–2030 Australian Cyber Security Strategy », Commonwealth of Australia, 2023, p. 30. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf. Consulté le 22 février 2024.

[1191] U.S. Department of the Treasury, « G7 Cyber Expert Group Recommends Action to Combat Financial Sector Risks from Quantum Computing », septembre 2024. https://home.treasury.gov/news/press-releases/jy2609. Consulté le 12 février 2025.

[1192] Kristen Csenkey et Nina Bindel, « Post-quantum cryptographic assemblages and the governance of the quantum threat », *Journal of Cybersecurity*, Vol. 9(1), 3 février 2023. https://academic.oup.com/cybersecurity/article/9/1/tyad001/7025478. Consulté le 2 janvier 2024.

[1193] Kaoru Kenyoshi et Hao Qin, « Framework of quantum key distribution (QKD) protocols in QKD network », ITU, 2024. https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18760. Consulté le 7 mars 2025.

défense et a adopté en 2023 la première stratégie quantique de l'Alliance[1194]. Celle-ci vise à rendre l'OTAN « quantum-ready », incluant l'adoption de cryptographie résistante aux ordinateurs quantiques pour sécuriser les communications et données militaires. L'OTAN encourage aussi la création d'une Communauté quantique transatlantique mobilisant gouvernements, industrie et monde académique, témoignant d'une approche coopérative entre alliés pour développer un écosystème quantique commun. Les États membres des Five Eyes (États-Unis, Royaume-Uni, Canada, Australie, Nouvelle-Zélande) promeuvent activement l'émergence de solutions post-quantiques, s'inscrivant dans une stratégie de défense commune via l'OTAN, AUKUS et Five Eyes pour maintenir leur avantage technologique face à ceux qu'ils désignent comme des « acteurs malveillants »[1195]. En parallèle, des regroupements non occidentaux comme les BRICS explorent leurs propres voies. La Chine et la Russie, en particulier, collaborent de plus en plus étroitement sur les technologies quantiques, cherchant à développer des communications inviolables indépendantes des Occidentaux. En 2023, des scientifiques chinois et russes ont ainsi testé avec succès une liaison quantique par satellite entre Moscou et Ürümqi, en Chine occidentale, présentée comme « inhackable » [1196]. Cette coopération sino-russe dans le quantique, potentiellement élargie à terme à d'autres pays BRICS, illustre la volonté de certains blocs de bâtir leurs propres écosystèmes sécuritaires quantiques, en marge des standards dominés par l'Occident.

L'Europe, quant à elle, développe une stratégie intégrée pour la sécurité quantique des données tout en affirmant sa souveraineté numérique. L'initiative Gaia-X, déjà citée précédemment, lancée en 2020, vise à créer une infrastructure européenne de données et de cloud souverain et sécuriser. Sans être spécifiquement quantique, Gaia-X pose un cadre où les données restent sous contrôle européen, ce qui facilitera à terme l'implémentation de solutions de chiffrement post-quantique certifiées en Europe. Sur le plan des communications, l'UE a déployé le projet EuroQCI (European Quantum Communication Infrastructure ou Infrastructure européenne de communication quantique) qui prévoit la mise en place d'un réseau quantique paneuropéen sécurisé. EuroQCI, développé avec 26 États membres et l'ESA, combinera une infrastructure fibre terrestre et des satellites quantiques pour assurer une couverture intégrale de l'UE et de ses territoires [1197]. Ce réseau, fondé sur la distribution quantique de clés, servira à protéger les communications des institutions gouvernementales et des infrastructures

---

[1194] NATO, « Summary of NATO's Quantum Technologies Strategy », 16 janvier 2024. https://www.nato.int/cps/en/natohq/official_texts_221777.htm. Consulté le 2 septembre 2024.

[1195] Dobson Baylee et Parsons Claire, « Outside the Atom: The Factors Governing the Five Eyes' Quantum Innovation », Queen's University, Vol. 9(7), 8 octobre 2024. https://www.queensu.ca/cidp/outside-atom-factors-governing-five-eyes-quantum-innovation. Consulté le 4 décembre 2024.

[1196] Weber Valentin, « The New Quantum Technology Race », International Politik Quarterly, 22 mars 2024. https://ip-quarterly.com/en/new-quantum-technology-race. Consulté le 3 avril 2024.

[1197] Commission Européenne, « Initiative relative à l'infrastructure européenne de communication quantique (EuroQCI) », juin 2019. https://digital-strategy.ec.europa.eu/fr/policies/european-quantum-communication-infrastructure-euroqci. Consulté le 21 janvier 2023.

critiques contre les cybermenaces présentes et futures. Le premier service visé est la distribution quantique de clés elle-même, avec un démonstrateur lancé en 2024 et un début de service opérationnel prévu pour 2027. Parallèlement, l'ENISA a publié des études pour guider la transition cryptographique. En 2022, elle soulignait la nécessité d'intégrer les systèmes post-quantiques dans les protocoles existants et d'anticiper les défis d'implémentation après la standardisation [1198]. En 2024, la Commission européenne a émis une recommandation encourageant les États membres à adopter une feuille de route coordonnée pour la migration vers la cryptographie post-quantique. Il s'agit ici d'harmoniser les calendriers et choix techniques au sein de l'UE, afin d'assurer une transition unifiée dans les administrations publiques et les infrastructures critiques, notamment via des schémas hybrides. Cette coordination européenne passe aussi par un groupe de coopération rassemblant les autorités nationales et l'ENISA, chargé d'évaluer et de sélectionner les algorithmes post-quantiques appropriés pour l'UE. La France, quant à elle, s'implique activement. Ainsi, l'ANSSI a publié dès 2022 un avis sur la migration vers la cryptographie post-quantique, préconisant une approche prudente via l'hybridation (combiner algorithmes actuels et post-quantiques) en attendant la maturation des standards [1199]. Des chercheurs français ont contribué de façon notable aux nouveaux standards puisqu'en mars 2025, le NIST américain a sélectionné le schéma de chiffrement HQC développé par des laboratoires à Limoges et Bordeaux comme standard mondial alternatif pour le chiffrement post-quantique[1200]. Cette réussite française dans la compétition NIST illustre la synergie possible entre coopération internationale en normalisation et souveraineté technologique, la France et l'Europe pouvant ainsi promouvoir des solutions nationales au rang de standards globaux.

La sécurisation post-quantique des données géographiques s'appuie également sur des efforts de normalisation conjointe entre les communautés géospatiales et de cybersécurité. Les organisations de normalisation, telles que l'ISO/TC 211 et l'OGC élaborent les standards qui assurent l'interopérabilité des systèmes d'information géographique. Jusqu'à présent, ces standards géospatiaux ont principalement traité de la structure des données, des métadonnées, et des services Web (catalogues, cartes en ligne, etc.), en laissant aux couches sous-jacentes le soin d'assurer la sécurité. Cependant, l'essor du cyberespace géographique et la criticité de ces données imposent désormais d'intégrer des

---

[1198] Enisa, « Post-Quantum Cryptography – Integration study », octobre 2022, p.4. https://www.enisa.europa.eu/sites/default/files/publications/Post%20Quantum%20Cryptography-%20Integration%20Publication.pdf. Consulté le 1er avril 2024.

[1199] Langlois-Berthelot Jean et Gaie Christophe, « Cryptographie : comment se protéger à l'ère quantique ? », Polytechnique Insight, 2024. https://www.polytechnique-insights.com/tribunes/geopolitique/cryptographie-comment-se-proteger-a-lere-post-quantique. Consulté le 23 février 2025.

[1200] Clim, « Le NIST (National Institute of Standards and Technology américain) consacre les chercheurs du Laboratoire Xlim (CNRS/Université de Limoges) et de l'Institut de mathématiques de Bordeaux (Bordeaux INP/CNRS/Université de Bordeaux) comme garants de la sécurité des échanges de données dans le monde entier. », CNRS et Université de Limoges, 11 mars 2025. https://www.unilim.fr/wp-content/uploads/sites/8/2025/04/DP_Standardisation-HQC.pdf. Consulté le 22 avril 2025.

exigences de sécurité plus strictes dans les normes. L'OGC a, par exemple, publié une spécification Web Services Security pour permettre aux services OGC d'annoncer leurs mécanismes de sécurité (authentification, contrôle d'accès, etc.) de manière interopérable. Ces services reposent sur HTTPS/TLS pour le transport des données géographique, de sorte que leur robustesse dépend directement des protocoles cryptographiques Internet. C'est ici qu'interviennent les recommandations post-quantiques du NIST et de l'IETF. À mesure que ces instances standardisent de nouveaux algorithmes et les intègrent dans des protocoles comme TLS, les services géospatiaux pourront les adopter pour rester sécurisés contre les attaques quantiques. L'IETF a déjà entamé des travaux pour définir des suites cryptographiques hybrides pour TLS et IKE (VPN) combinant algorithmes classiques et post-quantiques, ce qui bénéficiera in fine aux applications géospatiales en réseau. De son côté, l'ISO/IEC JTC 1 (informatique et techniques de sécurité) prépare l'adoption des algorithmes post-quantiques normalisés par le NIST en standards internationaux. Par exemple, l'ISO/IEC 23837-1:2023 vise à normaliser l'évaluation de la sécurité des systèmes QKD[1201], pendant que d'autres normes ISO porteront sur les schémas de cryptographie post-quantiques eux-mêmes. La coordination entre l'ISO/TC 211 et l'ISO/IEC JTC 1 devient cruciale pour que les standards géospatiaux intègrent les meilleures pratiques de cybersécurité post-quantique. Ainsi, un futur standard géospatial pourrait recommander qu'une infrastructure de données spatiales nationale utilise des algorithmes conformes aux standards NIST/ISO post-quantiques pour chiffrer ses échanges. De même, le W3C, via ses travaux sur le Web sémantique géospatial, veille à la compatibilité de ses protocoles avec les mécanismes de sécurité du Web, lesquels évolueront vers la post-quantique sans que les applications n'aient à en changer fondamentalement le design. En somme, une articulation progressive des référentiels géospatiaux avec les référentiels post-quantiques émanant du NIST, de l'IETF ou de l'ISO/IEC se dessine, afin de garantir à l'avenir que la chaîne complète, de la donnée géographique brute, jusqu'à son partage en ligne, reste robuste face aux menaces futures.

La géographie de la coopération quantique révèle donc des contrastes selon les régions et alliances technologiques. L'Amérique du Nord est en pointe sur la question via les États-Unis qui pilotent le mouvement avec le NIST et ont inscrit la migration post-quantique dans leur stratégie de cybersécurité nationale. Le Canada, membre du Five Eyes, coordonne étroitement avec Washington et Londres ces évolutions. De plus, via l'OTAN, les deux pays travaillent avec les Européens pour sécuriser les systèmes militaires, y compris les réseaux géospatiaux de l'Alliance par des méthodes « quantum-safe ». L'Europe de l'Ouest, notamment l'UE, privilégie une approche coopérative interne. Les États membres mutualisent la R&D en matière de technologie quantique tout en participant

[1201] ISO/IEC 23837-1:2023 Information security — Security requirements, test and evaluation methods for quantum key distribution. Part 1: Requirements. https://www.iso.org/standard/77097.html

activement aux programmes internationaux de normalisation. L'accent est mis sur la souveraineté européenne en matière de technologies critiques, ce qui explique l'investissement dans des solutions locales. L'Asie-Pacifique présente pour sa part un paysage contrasté. Le Japon est fortement intégré aux réseaux occidentaux, étant à la fois membre du QUAD, et un contributeur historique actif aux standards internationaux à l'ISO/IEC et l'UIT. La Corée du Sud et Singapour quant à eux ont des programmes avancés, souvent en partenariat avec l'UIT ou en suivant les normes NIST. Singapour a ainsi lancé le premier réseau quantique sécurisé d'Asie du Sud-Est et contribue aux standards UIT[1202]. L'Inde, elle, est membre du QUAD et multiplie les coopérations sur les technologies critiques avec les États-Unis et le Japon, tout en cherchant à développer ses propres capacités via un programme national quantique lancé en 2023[1203].

En Chine, Beijing investit énormément dans toutes les branches de la quantique et a déjà déployé des réseaux quantiques de télécommunication domestiques, comme le réseau QKD Beijing-Shanghai[1204], ainsi que son satellite quantique Micius[1205]. Sur le plan international, la Chine prône la coopération scientifique, elle a notamment réalisé des expériences QKD avec l'Autriche dès 2017[1206], mais, dans le contexte géopolitique actuel, elle tend à bâtir un écosystème fermé avec ses partenaires stratégiques comme la Russie, et les pays membres de l'initiative des Nouvelles routes de la Soie. La Russie, isolée des plateformes occidentales depuis 2022, se tourne vers la Chine pour la recherche quantique et pourrait adopter à terme des solutions de chiffrement quantique issues de ce partenariat plutôt que les standards NIST. Au Moyen-Orient et en Afrique, la plupart des pays ne disposent pas encore d'infrastructures quantiques significatives. Cependant, des États du Golfe, à l'instar des Émirats arabes unis, investissent dans ces technologies et pourraient servir de ponts entre fournisseurs occidentaux et asiatiques. De même, des organisations régionales pourraient émerger, par exemple, l'Union africaine pourrait à terme s'appuyer sur des partenariats avec l'UE pour introduire des solutions post-quantiques dans les réseaux de données africains, garantissant la sécurité des précieuses données géographiques. L'Amérique latine, enfin, commence à s'intéresser au sujet. Ainsi, le Brésil, membre des BRICS, participe aux discussions avec la Chine et la Russie sur les technologies

---

[1202] Haw Jing Yan et Hao Qin, « Driving towards standards for quantum key distribution », Center for Quantum technologies Singapore, 20 octobre 2023. https://www.cqt.sg/highlight/2023-10-qkd-standards/. Consulté le 12 février 2024.

[1203] Governement of India, « National Quantumn Mission (NQM) »n Ministry of Science and technology, mars 2023. https://dst.gov.in/national-quantum-mission-nqm. Consulté le 3 septembre 2024.

[1204] Chen, HZ., Li, MH., Wang, Y.Z. et al. « Implementation of carrier-grade quantum communication networks over 10000 km. », *npj Quantum* Inf, 11, 137 (2025). https://doi.org/10.1038/s41534-025-01089-8

[1205] Mazard Alexandra, « Lancement du premier satellite à communication quantique QUESS », France Diplomatie, 2 septembre 2016. Lancement du premier satellite à communication quantique QUESS - Ministère de l'Europe et des Affaires étrangères

[1206] « First Quantum Satellite Successfully Launched », Austrian Academy of Sciences. 16 Août 2016. https://www.oeaw.ac.at/en/events-communication/public-relations-communication/public-relations-communication/ausgewaehlte-oeaw-pressemeldungen/press-releases/first-quantum-satellite-successfully-launched/

émergentes, tout en collaborant avec l'UE via des projets Horizon Europe sur la cybersécurité. Le paysage de la standardisation des technologies quantiques présente donc un aspect fragmenté, avec d'un côté un bloc occidental misant sur des standards ouverts et une adoption coordonnée, un bloc sino-russe développant des solutions parallèles, et de nombreux pays en développement naviguant entre ces pôles en fonction des opportunités et alliances.

Ainsi, bien que la nécessité de coopérer soit largement reconnue, des fractures apparaissent selon les lignes de tension géopolitique, ce qui n'est pas sans conséquences sur la standardisation des données géospatiales. D'une part, les pays occidentaux et la Chine/Russie ne coopèrent que très marginalement sur la sécurité quantique, chacun craignant de dévoiler des avancées stratégiques à l'autre. Cette non-coopération se traduit par une possible balkanisation des normes. Les algorithmes post-quantiques recommandés par le NIST et l'ISO risquent de n'être adoptés que par les alliés des États-Unis, tandis que la Chine pourrait promouvoir ses propres algorithmes d'État, et ses protocoles QKD propriétaires, créant un écosystème alternatif. De même, la Russie développe une variante de GOST post-quantique.

Si de telles divergences persistent, l'interopérabilité des systèmes d'information géographique pourrait en souffrir. Par exemple, un service cartographique sécurisé avec un algorithme occidental pourrait ne pas être accessible à un client utilisant uniquement un algorithme chinois, et vice-versa. En outre, l'absence de coopération Sino-occidentale dans des enceintes comme l'ISO pourrait ralentir la mise à jour de certains standards globaux, chaque camp bloquant les propositions de l'autre, on a observé par le passé des frictions au sein de l'ISO sur l'inclusion de certaines primitives cryptographiques proposées par la Chine. D'autre part, cette fragmentation reflète des logiques de souveraineté informationnelle renforcées. En effet, chaque bloc estime crucial de maîtriser de bout en bout sa chaîne de sécurité des données sans dépendre d'acteurs extérieurs potentiellement hostiles. Ainsi, la Chine et la Russie considèrent le contrôle des techniques de chiffrement quantique comme indispensable pour protéger leurs données géospatiales contre toute ingérence occidentale. De même, l'Occident se prépare déjà à se prémunir contre d'éventuelles backdoors ou faiblesses délibérées dans des solutions quantiques chinoises. Le résultat est le renforcement de la fracture technologique Est/Ouest dans le cyberespace géospatial, chaque bloc cherchant l'autonomie totale de son cyberespace.

Néanmoins, il existe des espaces de dialogue, au premier lieu desquelles figurent les arènes de la normalisation internationales. Par exemple, l'UIT, en tant que plateforme onusienne inclusive, reste un lieu où les experts de tous pays codéveloppement certaines normes techniques, montrant qu'une coopération technique est encore possible malgré le climat stratégique tendu. Enfin, la fragmentation n'est pas seulement géopolitique, mais aussi économique, puisque les pays en développement risquent

d'être les perdants d'une absence de coopération, faute de moyens pour implémenter plusieurs standards concurrents.

En conclusion, la coopération internationale autour de la sécurité quantique des données géographiques se révèle indispensable, mais délicate. Elle emprunte des canaux multiples, alliances de défense, forums normatifs, partenariats scientifiques, pour tenter de maîtriser une transition technologique majeure qui ne connaît pas de frontières. Cette coopération est structurée par des alliances diverses (OTAN, UE, QUAD, Five Eyes) qui favorisent l'émergence de standards communs et le partage de bonnes pratiques post-quantiques[1207], mais elle est entravée par des logiques de puissance et de méfiance entre grands acteurs, pouvant mener à une fragmentation technique. Pour les données géospatiales, qui sont à la fois objet de souveraineté et biens échangés mondialement, le défi sera de préserver une interopérabilité et une résilience globales sans compromettre la sécurité de chacun. Les organisations internationales et organes de standardisation auront un rôle médian crucial pour arrimer l'écosystème géospatial aux avancées de la cryptographie post-quantique. La construction d'une sécurité post-quantique collaborative s'inscrit ainsi au cœur des enjeux de souveraineté numérique du XXIe siècle, intimement liée à la maîtrise du cyberespace et des données géographiques numériques. Les équilibres trouvés, ou manqués dans cette coopération internationale, conditionneront la capacité des nations à protéger leurs territoires numériques et à garantir la confiance dans les données géographiques à l'ère quantique. L'émergence annoncée de l'informatique quantique ne constitue donc pas seulement une révolution technologique, elle redéfinit en profondeur les paradigmes de sécurité sur lesquels reposent les systèmes d'information géographique et les infrastructures territoriales critiques. Cette transformation affecte directement la manière dont les données géographiques numériques, en tant qu'outils d'aide à la décision, sont protégées et mises en réseau dans le cyberespace.

Ainsi, les structures SIG sont aujourd'hui vulnérables face aux menaces liées aux futurs ordinateurs quantiques. Les algorithmes cryptographiques classiques qui garantissent la confidentialité, l'authenticité et l'intégrité des données, qu'il s'agisse d'un fichier cadastral, d'une base de données topographiques ou de flux de données de capteurs en temps réel, risquent de devenir obsolètes. Cette vulnérabilité structurelle, couplée à l'interconnexion croissante des territoires et à la dépendance aux plateformes cloud, expose les systèmes d'informations géographiques à un risque qui ne peut être ignoré.

[1207] Kristen Csenkey et Nina Bindel, « Post-quantum cryptographic assemblages and the governance of the quantum threat », *Journal of Cybersecurity*, Vol. 9(1), 3 février 2023. https://academic.oup.com/cybersecurity/article/9/1/tyad001/7025478. Consulté le 2 janvier 2024.

Face à cette menace, la normalisation sera amenée à jouer un rôle crucial en participant à diffuser des algorithmes post-quantiques capables de résister aux attaques des ordinateurs quantiques. C'est également via les instances internationales de normalisation que pourra se faire l'implémentation de ces mêmes algorithmes au sein des infrastructures de données géographiques, qu'elles soient civiles ou militaires. Cependant, cette coopération s'inscrit dans un contexte géopolitique fracturé, marqué par la montée des tensions technologiques et par un risque de fragmentation normative croissant. Ce risque est double, tout d'abord celui d'une balkanisation des standards cryptographiques, sapant l'interopérabilité mondiale, et celui d'un creusement des inégalités en matière d'accès et de diffusion des données géographiques, entre les pays dotés d'une capacité souveraine de transition post-quantique et ceux laissés à la marge de ces mutations. Ainsi, la standardisation des technologies quantiques met en lumière les rapports de pouvoir au sein du cyberespace, dans lequel les données géographiques jouent un rôle central, en tant que représentations normées de l'espace, mais aussi comme outils d'aide à la décision. Dans cette perspective, la France et l'Union européenne doivent chercher à se positionner comme architectes d'un cyberespace géographique résilient, interopérable et souverain, en participant activement à ces échanges, et en défendant une vision éthique de la sécurité territoriale. Face à cet écosystème en mutation, il est essentiel d'anticiper les mutations possibles de l'environnement normatif international dans le domaine des données géographiques.

Conclusion du chapitre VIII

Plusieurs constats majeurs s'imposent à la suite de ce chapitre, qui éclairent la reconfiguration en cours des rapports de pouvoir dans le cyberespace territorial. La première partie a démontré que l'intelligence artificielle et la blockchain constituent désormais des terrains de normalisation à part entière, où se jouent des enjeux de souveraineté aussi décisifs que ceux identifiés pour les formats de données classiques. Les standards de données sémantiques, tels que JSON-LD, GeoJSON-LD et GeoSPARQL forment l'infrastructure normative sans laquelle le potentiel de l'intelligence artificielle appliquée aux données géographiques ne pourrait être pleinement exploité. Ces formats constituent le langage commun permettant aux algorithmes d'apprentissage automatique de traiter l'information territoriale, de la cartographie automatisée à l'urbanisme prédictif, du renseignement d'origine image à l'aide à la décision tactique. Parallèlement, la blockchain offre un potentiel considérable pour certifier l'authenticité et l'intégrité des données géographiques dans un contexte où la manipulation de l'information territoriale devient un enjeu de guerre informationnelle. Les expérimentations menées en Géorgie, en Suède, au Ghana ou au sein de l'armée française avec le projet FIBR2EO attestent de la maturité croissante de ces applications. Toutefois, l'analyse a également révélé les défis éthiques et réglementaires transversaux que soulèvent ces technologies : biais algorithmiques, opacité des systèmes d'apprentissage profond, tension entre immuabilité de la blockchain et droit à l'oubli du RGPD, émergence de modèles concurrents de diplomatie normative entre l'Europe, les États-Unis et la Chine.

La deuxième partie a montré que les jumeaux numériques territoriaux et les métavers géographiques constituent la synthèse opérationnelle de ces briques élémentaires, mobilisant simultanément standards de données, intelligence artificielle, mécanismes de certification et cadres réglementaires. Cette intégration amplifie considérablement les enjeux de normalisation identifiés précédemment. Un jumeau numérique urbain doit assembler des données provenant de sources multiples et hétérogènes, dont la compatibilité suppose une normalisation rigoureuse à tous les niveaux : technique, matériel, logiciel, sémantique, interactionnel et cartographique. Les environnements immersifs posent des défis supplémentaires d'interopérabilité, les plateformes de réalité augmentée utilisant des approches propriétaires peu compatibles. La bataille entre formats ouverts et formats propriétaires, déjà analysée pour les données géospatiales classiques, se rejoue dans l'univers des métavers. Par ailleurs, les cybermenaces spécifiques qui pèsent sur ces systèmes cyber-physiques prennent une dimension nouvelle. Toute faille informatique dans un jumeau numérique pilotant des infrastructures critiques peut avoir des répercussions concrètes sur le fonctionnement du territoire réel.

La troisième partie a établi que l'émergence de l'informatique quantique constitue une rupture paradigmatique qui menace l'ensemble de l'édifice normatif et technique construit dans les parties précédentes. Les algorithmes cryptographiques classiques qui garantissent la confidentialité, l'authenticité et l'intégrité des données géospatiales sont appelés à devenir obsolètes à l'horizon 2030-2035. Cette vulnérabilité structurelle, couplée à la stratégie « stocker maintenant, déchiffrer plus tard » déjà mise en œuvre par certains acteurs étatiques, fait peser un risque immédiat sur les informations territoriales sensibles à longue durée de vie. Les efforts de normalisation de la cryptographie post-quantique engagés par le NIST, l'ISO, l'IETF et l'ETSI ouvrent la voie à une transition vers des algorithmes résistants aux attaques quantiques tels que CRYSTALS-Kyber, CRYSTALS-Dilithium ou HQC. Toutefois, cette transition ne se réduit pas à une simple évolution technique, elle constitue un enjeu géopolitique majeur où se confrontent des visions concurrentes de la souveraineté numérique. La géographie de la coopération quantique révèle une fragmentation croissante entre le bloc transatlantique misant sur des standards ouverts coordonnés, le bloc sino-russe développant des solutions parallèles au sein d'un écosystème fermé, et de nombreux pays émergents ou en développement naviguant entre ces pôles au gré des opportunités et des alliances.

Au-delà de ces constats sectoriels, ce chapitre met en lumière plusieurs dynamiques transversales qui structurent la reconfiguration des rapports de pouvoir dans le cyberespace géospatial. La première dynamique est celle de l'accélération technologique et de ses implications normatives. Le rythme d'innovation dans les domaines de l'intelligence artificielle, de la blockchain, des jumeaux numériques et de l'informatique quantique dépasse largement la capacité des organismes de normalisation traditionnels à produire des standards consensuels. Cette accélération favorise l'émergence de normes de facto imposées par les acteurs technologiques dominants, au détriment des processus multilatéraux ouverts. Elle crée également une asymétrie croissante entre les pays capables de participer à la définition des standards et ceux contraints de les adopter sans avoir contribué à leur élaboration.

La deuxième dynamique est celle de la convergence des technologies et de l'amplification des interdépendances. Les systèmes géospatiaux contemporains ne peuvent plus être analysés comme des assemblages de composants indépendants. L'intelligence artificielle dépend des standards de données sémantiques, les jumeaux numériques mobilisent simultanément IA et blockchain, la sécurité de l'ensemble repose sur des primitives cryptographiques dont la robustesse conditionne la confiance dans le système global. Cette convergence signifie qu'une vulnérabilité dans un maillon de la chaîne peut compromettre l'intégrité de l'ensemble, comme l'illustre la menace quantique sur les fondations cryptographiques de la blockchain et de l'IA géospatiale.

La troisième dynamique est celle de la territorialisation du cyberespace et de la souveraineté numérique. Loin de l'utopie d'un cyberespace sans frontières, les technologies analysées dans ce chapitre révèlent au contraire une territorialisation croissante des infrastructures numériques. Les jumeaux numériques sont ancrés dans des territoires physiques dont ils reproduisent la géographie. Les systèmes de positionnement par satellite demeurent sous contrôle étatique ou régional. Les données d'entraînement des modèles d'intelligence artificielle géospatiale reflètent les biais et les priorités de leurs concepteurs. Les choix de standards cryptographiques engagent la souveraineté à long terme. Cette territorialisation fait de la normalisation des données géographiques un enjeu de puissance où se redéfinissent les contours de l'autonomie stratégique.

En définitive, le chapitre VIII démontre que les technologies émergentes ne constituent pas simplement des outils au service de la géomatique, elles reconfigurent en profondeur les rapports de pouvoir entre États, entre blocs géopolitiques, entre acteurs publics et privés, dans la production, le contrôle et la sécurisation de l'information géographique. La maîtrise de ces technologies et de leurs standards associés devient un attribut de souveraineté aussi déterminant que la maîtrise des territoires physiques qu'elles représentent et transforment. Les analyses conduites dans ce chapitre sur les technologies émergentes et leurs implications normatives ouvrent nécessairement sur une interrogation prospective. Les dynamiques identifiées, qu'il s'agisse de l'accélération technologique, de la convergence des systèmes, de la fragmentation géopolitique ou de la territorialisation du cyberespace, dessinent des trajectoires dont l'aboutissement demeure incertain. Plusieurs futurs sont possibles, et leur réalisation dépendra des choix politiques et des rapports de force qui façonneront les prochaines décennies.

Le chapitre suivant se propose d'explorer ces futurs possibles en adoptant une démarche prospective structurée. Trois scénarios méritent une attention particulière. Le premier scénario est celui d'une fragmentation normative mondiale où le découplage technologique entre grandes puissances conduirait à l'émergence de sphères d'influence incompatibles. Dans cette hypothèse, le monde ne convergerait pas vers des standards techniques universels, mais se diviserait en blocs géopolitiques promouvant chacun leurs propres normes en matière de formats de données, de protocoles, d'algorithmes d'intelligence artificielle et de cryptographie. L'interopérabilité des systèmes géospatiaux mondiaux en souffrirait gravement, contraignant chaque pays à un choix d'allégeance technologique ou à un coûteux double emploi des systèmes concurrents.

Le deuxième scénario est celui d'une gouvernance multilatérale renforcée où les organismes internationaux de normalisation parviendraient à préserver un socle commun de standards interopérables malgré les tensions géopolitiques. Dans cette hypothèse, les grandes puissances reconnaîtraient leur intérêt mutuel à maintenir des infrastructures géospatiales interconnectées pour la

gestion des défis globaux tels que le changement climatique, les crises humanitaires ou la régulation du trafic aérien et maritime. La normalisation resterait un espace de coopération technique au sein duquel les rivalités politiques seraient partiellement mises entre parenthèses.

Le troisième scénario est celui d'une différenciation régionale maîtrisée où l'Union européenne parviendrait à affirmer une voie propre entre l'hégémonie américaine et l'autonomisation chinoise. Dans cette hypothèse, l'Europe développerait une souveraineté numérique fondée sur des standards ouverts, mais certifiés, une régulation exigeante en matière de protection des données et d'éthique algorithmique, et une capacité industrielle autonome dans les technologies critiques. La France, forte de son expertise en géomatique, en cryptographie et en intelligence artificielle, jouerait un rôle moteur dans cette stratégie européenne.

Ces scénarios ne sont pas mutuellement exclusifs. L'avenir sera probablement fait de combinaisons et de transitions entre ces différentes trajectoires. Le chapitre IX s'attachera à les explorer en détail, en analysant les facteurs qui pourraient favoriser l'une ou l'autre de ces évolutions, les conséquences pour la France et l'Europe, et les recommandations qui peuvent en être tirées pour les acteurs de la normalisation géospatiale. Car si l'avenir reste ouvert, il n'est pas pour autant indéterminé. En effet, les choix effectués aujourd'hui dans les arènes de la normalisation, les investissements consentis dans les technologies émergentes, les alliances nouées entre États et entre organisations façonneront les contours du cyberespace géographique de demain et, avec lui, les conditions de la souveraineté territoriale à l'ère numérique.

Chapitre IX – Quel avenir pour la normalisation des données géographiques ?

Les chapitres précédents ont analysé les dynamiques contemporaines de la normalisation des données géographiques numériques, à la fois la structuration institutionnelle des organismes de standardisation, les rapports de force entre puissances dans les arènes normatives, l'impact des technologies émergentes sur les équilibres établis, et les enjeux de souveraineté qui traversent l'ensemble de ces processus. Ces analyses ont révélé un écosystème en mutation profonde, travaillé par des tensions contradictoires entre ouverture et contrôle, entre coopération internationale et affirmation des souverainetés nationales, entre standards ouverts et formats propriétaires, entre logiques techniques et logiques politiques. Le présent chapitre adopte une perspective différente en se projetant dans l'avenir. La démarche prospective ne consiste pas à prédire ce qui adviendra, mais elle vise plutôt à explorer les futurs possibles, à identifier les trajectoires que dessinent les tendances actuelles, à analyser les bifurcations qui pourraient infléchir ces trajectoires, et à éclairer les choix qui s'offrent aux acteurs de la normalisation géospatiale. En ce sens, la prospective se veut avant tout un outil d'aide à la décision stratégique. Trois questions structurent cette exploration prospective. La première porte sur l'architecture globale du système normatif. Ainsi, assisterons-nous à une fragmentation du monde en blocs technologiques incompatibles, ou les forces de l'interdépendance parviendront-elles à préserver un socle commun de standards interopérables ? La deuxième question concerne les stratégies des acteurs : comment les États, les entreprises, les consortiums et les communautés scientifiques peuvent-ils peser sur l'évolution des normes pour défendre leurs intérêts et leurs valeurs ? La troisième question touche aux domaines spécifiques où se jouera l'avenir de la normalisation géospatiale. Quels enjeux émergents, de la défense à l'environnement, des smart cities à l'exploration spatiale, façonneront les standards de demain ?

Ces trois questions correspondent aux trois parties qui structurent ce chapitre. La première partie examine le scénario d'une fragmentation normative mondiale, où le découplage technologique entre grandes puissances conduirait à l'émergence de sphères d'influence incompatibles. Ce scénario, parfois qualifié de « splinternet » ou de balkanisation numérique, constitue l'horizon le plus préoccupant pour l'interopérabilité des systèmes géospatiaux. Il convient d'en analyser les facteurs, les manifestations possibles et les conséquences pour les différents acteurs. La deuxième partie s'intéresse aux stratégies d'influence que peuvent déployer les acteurs publics et privés pour orienter l'évolution des normes. Elle examine successivement la diplomatie normative des États, les innovations

stratégiques des consortiums privés et le rôle des alliances entre universités et industries dans l'élaboration des standards. La troisième partie se projette dans les domaines d'application où se joueront les batailles normatives de demain, avec une attention particulière pour le secteur de la défense où les enjeux de souveraineté sont les plus aigus.

Tout au long de ce chapitre, la France et l'Union européenne serviront de fil conducteur. Non par européocentrisme, mais parce que la position européenne dans la géopolitique des normes présente une singularité qui mérite attention. Située entre l'hégémonie technologique américaine et la montée en puissance chinoise, l'Europe tente aujourd’hui de définir une troisième voie fondée sur des standards ouverts, mais souverains, une régulation exigeante, mais favorable à l'innovation, une coopération internationale, mais préservant l'autonomie stratégique. Le succès ou l'échec de cette stratégie européenne, dans laquelle la France joue un rôle moteur, conditionnera en partie l'avenir de la normalisation géospatiale mondiale. La prospective comporte une dimension normative assumée. Décrire les futurs possibles, c'est aussi implicitement désigner ceux qui sont souhaitables et ceux qui doivent être évités. Le scénario d'une fragmentation normative mondiale, s'il devait se réaliser, constituerait une régression considérable pour la coopération scientifique, la gestion des défis environnementaux globaux et la circulation des connaissances géographiques. À l'inverse, le maintien d'un cadre normatif interopérable, même imparfait, préserverait les acquis de plusieurs décennies de standardisation patiente. Entre ces deux extrêmes, de multiples configurations intermédiaires sont envisageables, combinant fragmentation dans certains domaines et coopération dans d'autres, rivalité entre blocs et alliances de circonstance. C'est dans cet espace des possibles que se déploie l'analyse prospective du présent chapitre.

1. Vers une fragmentation normative mondiale ?

Le premier scénario prospectif qu'il convient d'examiner est celui d'une fragmentation des normes internationales en matière de données géographiques numériques. Ce scénario, le plus disruptif pour l'ordre normatif actuel, mérite une analyse approfondie tant les signaux qui l'annoncent se multiplient dans le contexte géopolitique contemporain.

L'hypothèse centrale de ce scénario est la suivante : le monde ne convergerait pas vers des standards techniques universels, mais se diviserait en sphères technologiques distinctes alignées sur de grands blocs géopolitiques concurrents. Les États-Unis, la Chine, la Russie, l'Union européenne et potentiellement d'autres pôles régionaux développeraient chacun leurs propres écosystèmes normatifs, partiellement ou totalement incompatibles entre eux. Cette évolution s'inscrirait dans le prolongement des tensions actuelles dans le cyberespace, où l'on observe déjà la fracture d'un paysage technologique autrefois relativement intégré le long de lignes géopolitiques.

Une telle fragmentation ne serait pas sans précédent historique. Le XXe siècle a connu des périodes où les systèmes techniques des différents blocs étaient largement incompatibles, comme les standards ferroviaires distincts entre l'Europe occidentale et l'URSS, des systèmes électriques divergents, et des normes de télécommunication séparées. La mondialisation des dernières décennies avait semblé dépasser ces clivages en instaurant des standards techniques universels, du moins dans le domaine numérique. Internet, le GPS, les formats de données géospatiales de l'OGC constituaient autant de « biens communs normatifs » partagés par l'ensemble de la planète. C'est précisément cet acquis qui pourrait être remis en cause dans le scénario de fragmentation. Plusieurs facteurs structurels alimentent cette dynamique de découplage. Le premier est la montée du technonationalisme, doctrine selon laquelle la maîtrise des technologies clés constitue un attribut essentiel de la puissance et de la souveraineté nationale. Cette doctrine, longtemps cantonnée aux secteurs militaires, s'étend désormais à l'ensemble des technologies numériques, des semi-conducteurs à l'intelligence artificielle, des systèmes de positionnement par satellite à la cryptographie post-quantique. Le deuxième facteur est l'intensification de la rivalité sino-américaine, qui structure de plus en plus les relations internationales selon une logique de compétition systémique. Cette rivalité se traduit par des mesures de découplage technologique telles que les restrictions d'exportation de semi-conducteurs, les interdictions d'équipements réseau et les contrôles sur les investissements dans les technologies sensibles qui fragmentent les chaînes de valeur mondiales. Le troisième facteur est la quête d'autonomie numérique de puissances comme la Russie, accélérée par les sanctions internationales consécutives à l'invasion de l'Ukraine, qui pousse ces pays à développer des alternatives aux technologies et standards occidentaux.

Dans le domaine géospatial, la fragmentation normative pourrait affecter l'ensemble de la chaîne de valeur de l'information géographique. Les formats de données, aujourd'hui largement harmonisés autour des standards OGC et ISO, pourraient diverger entre blocs promouvant chacun leurs propres spécifications. Les systèmes de positionnement par satellite, déjà pluriels avec le GPS américain, le Galileo européen, le GLONASS russe et le BeiDou chinois, pourraient voir leurs protocoles de communication et leurs mécanismes d'authentification devenir incompatibles. Les plateformes d'intelligence artificielle géospatiale, les infrastructures de certification blockchain, les algorithmes de cryptographie post-quantique pourraient suivre des trajectoires distinctes selon les blocs, créant des « murs technologiques » entravant la circulation des données et des services géographiques. Les conséquences d'une telle fragmentation seraient considérables. L'interopérabilité des systèmes géospatiaux mondiaux, fruit de décennies de standardisation patiente, serait gravement compromise. Les acteurs souhaitant opérer à l'échelle mondiale devraient maintenir des systèmes multiples, multipliant les coûts et les complexités. La coopération scientifique internationale dans les domaines qui requièrent des données géographiques globales, du changement climatique à la gestion des catastrophes naturelles, serait entravée. Les pays du Sud global, incapables de maintenir plusieurs écosystèmes normatifs parallèles, seraient contraints à des choix d'allégeance technologique lourds de conséquences pour leur souveraineté.

La présente partie examine ce scénario de fragmentation selon plusieurs angles. Elle analyse d'abord les lignes de fracture politico-techniques qui pourraient conduire à cette fragmentation, en distinguant les clivages sino-américain, la position singulière de la Russie, le rôle de l'Union européenne et les stratégies des puissances émergentes. Elle examine ensuite les domaines techniques les plus susceptibles d'être affectés, qu'il s'agisse des formats de données géographiques, des systèmes de certification et blockchain, de l'intelligence artificielle géospatiale, ou encore de la cybersécurité et de la cryptographie post-quantique. Elle évalue enfin les conséquences pour l'interopérabilité des systèmes géospatiaux et les stratégies d'adaptation que pourraient déployer les différents acteurs face à ce morcellement.

Cette analyse ne présuppose pas que le scénario de fragmentation soit inéluctable. Des forces contraires, tenant à l'interdépendance économique, aux besoins de coopération face aux défis globaux et à l'inertie des systèmes techniques existants, pourraient préserver un socle minimal d'interopérabilité. L'objectif est plutôt d'explorer les implications d'une trajectoire de fragmentation pour mieux identifier les points de vigilance et les leviers d'action susceptibles de l'infléchir. Car si l'avenir n'est pas écrit, les choix effectués aujourd'hui dans les arènes de la normalisation contribueront à déterminer lequel des futurs possibles deviendra réalité.

1.1. La possibilité d'un découplage normatif à l'échelle mondiale

Plusieurs clivages géopolitiques actuels laissent présager un monde fragmenté en blocs normatifs. Le premier oppose le bloc occidental mené par les États-Unis et le bloc eurasiatique mené par la Chine, sur fond de compétition technologique stratégique. À cela s'ajoutent la posture de la Russie, engagée dans une quête d'autonomie numérique accélérée par les sanctions internationales, le rôle singulier de l'Union européenne en tant que « superpuissance réglementaire » globale, ainsi que les aspirations des puissances émergentes comme l'Inde, les pays de l'ASEAN, ou encore le Brésil, et du Sud global à ne pas être de simples spectateurs de cette rivalité. États-Unis et Chine cristallisent aujourd'hui la rivalité normative. Les États-Unis ont historiquement dominé l'écosystème des standards Internet et géospatial. Cependant, la Chine déploie depuis une décennie une stratégie proactive de définition de normes alternatives, consciente du caractère stratégique de ce levier. Beijing a mesuré l'importance stratégique de l'élaboration et de l'imposition de normes techniques liées à Internet et entend peser sur les standards technologiques du futur. Concrètement, la Chine investit et participe activement aux instances de normalisation afin de promouvoir ses solutions [1208]. Se développe ainsi une dynamique de « guerre des standards » où chaque camp cherche à diffuser ses protocoles, ses plateformes et ses référentiels technologiques auprès de ses alliés et partenaires.

Du côté américain, la réaction a consisté à durcir les contrôles technologiques, en imposant des restrictions sur l'exportation de semi-conducteurs avancés, ou en imposant des sanctions contre Huawei comme cela avait été fait en 2019[1209], et à s'assurer du soutien de pays alliés pour adopter les standards occidentaux. Washington s'efforce de préserver un Internet mondial ouvert selon son modèle, tout en excluant les équipements ou logiciels perçus comme des chevaux de Troie chinois. Cette polarisation s'étend aux technologies émergentes. À titre d'exemple, dans l'IA géospatiale, se développe de plus en plus des « écosystèmes IA » distincts (les grands modèles d'IA entraînés sur des données occidentales d'un côté, et des modèles équivalents entraînés sur des données chinoises de l'autre), accompagnés de cadres éthiques divergents. Certains observateurs évoquent même le risque d'un « rideau de fer de l'IA », où le monde serait scindé en blocs technologiques étanches dominés par les grandes puissances

[1208] Nocetti Julien, « Un Internet en morceaux ? Fragmentation d'Internet et stratégies de la Chine, la Russie, l'Inde et l'Union européenne », Ifri, 27 octobre 2025. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_nocetti_fragmentation_internet.pdf. Consulté le 15 janvier 2025.

[1209] En 2019, le gouvernement américain a sanctionné Huawei pour avoir fait des affaires avec des adversaires, tels que l'Iran, en prenant des mesures judiciaires et en ajoutant l'entreprise à la liste des entités du Bureau de l'industrie et de la sécurité (BIS) du ministère du Commerce, dans le but de paralyser Huawei en perturbant sa chaîne d'approvisionnement. Rodrigo Balbontin, « Backfire: Export Controls Helped Huawei and Hurt U.S. Firms », Information Technology & Innovation Foundation, 27 octobre 2025. https://itif.org/publications/2025/10/27/backfire-export-controls-helped-huawei-and-hurt-us-firms/. Consulté le 15 janvier 2025.

et leurs entreprises, aux dépens des pays tiers [1210]. Cette idée traduit la crainte de voir les flux de connaissances, de matériels et de données liés à l'IA se bloquer entre l'Est et l'ouest, formant des silos technologiques incompatibles. En somme, la rivalité sino-américaine dessine un bipolarisme technologique avec d'un côté, un écosystème mené par les GAFAM et encadré par les régulateurs occidentaux, de l'autre, un écosystème mené par les BATX (Baidu, Alibaba, Tencent, Xiaomi, etc.) et piloté de près par l'État chinois. Dans un scénario de fragmentation exacerbée, ces deux écosystèmes établiraient des normes incompatibles dans de nombreux domaines, forçant chaque pays à un choix d'allégeance technologique ou à un difficile double emploi des deux systèmes.

La Russie se positionne également comme un pôle de fragmentation normative, quoique de moindre poids économique que les deux précédents. Depuis le milieu des années 2010, Moscou a affiché la doctrine d'un « Internet souverain », cherchant à se doter d'une infrastructure nationale capable de fonctionner de manière isolée du réseau mondial en cas de besoin. Cette vision s'est traduite par des mesures concrètes telles que le routage national du trafic, la valorisation d'alternatives nationales comme le moteur de recherche Yandex, ou le système de navigation GLONASS en alternative au GPS, une loi imposant le stockage des données personnelles des citoyens russes sur des serveurs localisés en Russie, et des tests réguliers de déconnexion de l'internet russe du reste du monde. La guerre en Ukraine (depuis 2022) et les sanctions occidentales qui l'ont accompagnée ont joué un rôle d'accélérateur. L'exode ou le blocage de nombreuses entreprises technologiques occidentales hors de Russie a forcé le pays à pousser plus avant son autonomie numérique. Se sont également développés des systèmes d'exploitation nationaux (Astra Linux, etc.), de magasins d'applications alternatifs (RuStore pour Android), et plus globalement un effort national pour rediriger le trafic Internet via des infrastructures contrôlées localement. La Russie justifie ces mesures par la nécessité de se prémunir contre les ingérences et blackouts potentiels orchestrés de l'extérieur. Cependant, ce faisant, elle contribue à morceler davantage l'Internet mondial. La continuité du réseau global s'en trouve fragilisée, comme le note une étude de l'IFRI : dans des pays comme la Chine ou la Russie, *« le contrôle étatique du réseau tend à fragiliser sa continuité et augmente fortement les risques pour les populations concernées »*[1211] en termes de censure et d'atteinte aux droits. En matière de normes, Moscou s'aligne fréquemment sur Beijing pour promouvoir une gouvernance d'Internet plus étatique au sein des enceintes internationales. Par exemple, la Russie a appuyé l'initiative chinoise « New IP » à l'UIT et milite pour une plus grande influence des États dans les organes de standardisation. On peut

[1210] Kai-Hsin Hung, « Beyond Big Tech Geopolitics Moving towards local and people-centred artificial intelligence », tni, 4 février 2025. https://www.tni.org/en/article/beyond-big-tech-geopolitics. Consulté le 6 mai 2025.

[1211] Nocetti Julien, « Un Internet en morceaux ? Fragmentation d'Internet et stratégies de la Chine, la Russie, l'Inde et l'Union européenne », Ifri, février 2014, p.6. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_nocetti_fragmentation_internet_2024.pdf. Consulté le 23 février 2025.

donc imaginer, dans un scénario de blocs, un axe sino-russe de normes technologiques partageant une philosophie commune, bien que la Russie, en réalité, dépende largement de la Chine pour de nombreux équipements et savoir-faire numériques faute d'une base industrielle équivalente. Une telle alliance serait profondément déséquilibrée et le conflit ukrainien en consumant les ressources de la Russie, semble devoir renforcer ce déséquilibre à l'avantage de Beijing, qui dans les faits contrôlerait largement une telle alliance technologique.

L'Union européenne occupe ici une position ambivalente. D'une part, l'Europe reste, tout du moins pour le moment, relativement aligné avec les États-Unis sur le plan géopolitique, mais d'autre part, elle cherche à tracer une troisième voie en matière de régulation du numérique, souvent centrée sur la défense de ses valeurs et de sa souveraineté numérique. L'UE s'est ainsi distinguée comme une « superpuissance réglementaire », capable d'imposer mondialement des normes via le fameux Brussels effect [1212]. Des règlements, comme le RGPD ou, plus récemment, le Digital Markets Act et le Digital Services Act, fixent des standards de fait que les grandes plateformes doivent appliquer bien au-delà du seul territoire européen. De même, dans le domaine des informations géographiques, l'UE a impulsé dès 2007 la directive INSPIRE, un ambitieux cadre de standardisation et d'interopérabilité des données géographiques à l'échelle du continent, qui s'est érigé en référence internationale. Cette capacité à produire et déployer des normes à l'échelle mondiale demeure la principale force politique de l'UE. Face à la fragmentation, l'UE a choisi d'adopter une stratégie particulière, elle tente de contrer la tendance en promouvant l'universalisation de ses normes. Comme le souligne le chercheur Julien Nocetti, l'Europe *« mène une politique qui vise précisément à contrer la tendance mondiale à la fragmentation dans le champ du numérique et des télécommunications »*[1213]. Le développement par l'Europe du système Galileo, tout en gardant son système ouvert et interopérable avec les autres États, confirme cette stratégie de protection de ses intérêts alliés à une volonté d'ouverture et de maintien de la libre concurrence. L'UE investit également dans des infrastructures et standards ouverts. L'objectif est double, réduire sa dépendance aux technologies extra-européennes tout en évitant un éclatement du cyberespace qui nuirait à ses intérêts économiques et démocratiques. Néanmoins, si les rapports de force globaux se crispent, l'Europe pourrait se retrouver sous pression de choisir un camp ou de voir ses normes contestées par les blocs rivaux. Il faut noter également que l'UE cherche également à entraîner d'autres acteurs dans son sillage réglementaire en misant notamment sur le caractère attractif et exportable de ses normes pour fédérer autour d'elles. À titre d'exemple, plusieurs pays d'Afrique ou

[1212] Bradford Anu, « The Brussels Effect : How the European Union Rules the World », Oxford University Press, 2020, pp. 833-838.; Meyer Zach, « In tech, the death of the Brussels effect is greatly exaggerated », 8 décembre 2023. https://www.cer.eu/insights/tech-death-brussels-effect-greatly-exaggerated#. Consulté le 15 janvier 2024.

[1213] Nocetti Julien, « Un Internet en morceaux ? Fragmentation d'Internet et stratégies de la Chine, la Russie, l'Inde et l'Union européenne », Ifri, février 2014, p.33. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_nocetti_fragmentation_internet_2024.pdf. Consulté le 23 février 2025.

d'Amérique latine se sont inspirés du RGPD pour leurs lois nationales. À l'ONU, l'UE promeut une initiative de « diplomatie du numérique » afin d'éviter un schisme de l'Internet. Reste à savoir si cela suffira à endiguer les forces de fragmentation, surtout si les États-Unis ou la Chine ne s'y rallient pas pleinement.

Entre ces pôles, de nombreux pays émergents ou en développement refusent l'idée d'avoir à choisir purement et simplement entre deux modèles imposés. Leur objectif est d'exercer une autonomie stratégique dans le numérique, en piochant le meilleur de chaque camp ou en développant leurs propres solutions locales. Certains chercheurs y voient ici une forme de réactualisation du mouvement des Non-Alignés à l'ère digitale [1214]. Ainsi, l'Inde, forte de son marché de 1,4 milliard d'habitants et de son vivier technologique, illustre cette approche. Longtemps non alignée géopolitiquement, l'Inde pratique aujourd'hui un « mix stratégique ». Ainsi, elle coopère étroitement avec les États-Unis sur certains aspects (intégration dans le Quad, accueil de data centers d'entreprises américaines, adoption d'une partie des standards occidentaux), tout en développant simultanément des partenariats technologiques avec la Russie et surtout avec la Chine (dans les domaines de l'énergie et des technologies spatiales). New Delhi vise en réalité une véritable souveraineté numérique indienne : programmes de localisation des données, préférence nationale pour certains marchés publics IT, réseau de navigation indien (NavIC), normes indiennes pour la 5G, notamment le standard 5Gi proposé par l'Inde pour s'adapter aux zones rurales[1215]. Ainsi, dans un scénario de fragmentation par blocs, l'Inde chercherait vraisemblablement à ne pas s'enfermer dans un camp unique. Elle pourrait adhérer partiellement aux standards de chaque bloc selon ses intérêts, voire proposer des normes alternatives émanant du Sud. Néanmoins, son degré d'indépendance effective dépendra de ses capacités internes à produire les technologies clés sans toujours devoir importer.

En Asie du Sud-Est, les pays de l'ASEAN adoptent une démarche similaire, bien que leur hétérogénéité interne soit grande. Globalement, ces pays tirent profit à la fois de l'investissement technologique chinois et de l'écosystème occidental. Conscients du déséquilibre actuel du pouvoir numérique, où 68 % des data centers mondiaux sont contrôlés par des géants américains ou européens, contre 26 % en Asie[1216], les États d'Asie du Sud-Est multiplient les initiatives pour rapatrier une partie de la valeur numérique chez eux. *« La maîtrise des données est une question de souveraineté*

[1214] Latha Reddy et Anoushka Soni, « Is There Space for a Digital Non-Aligned Movement? », in *New Conditions and Constellations in Cyber*, Cyberstability Paper Series, The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace , 2021. https://hcss.nl/wp-content/uploads/2021/09/Is-There-Space-for-a-Digital-Non-Aligned-Movement.pdf. Consulté le 10 mars 2024.

[1215] Ashok Kumar, « India's Own 5G Technology – 5Gi », National Telecommunications Institute for Policy Research, Innovations & Training (NTIPRIT), 2015. https://ntiprit.gov.in/pdf/gsm2g/All_about_Indias_own_5G_called_5Gi.pdf. Consulté le 15 mai 2025.

[1216] Vishal Rana et Govand Khalid Azeez, « Southeast Asia's Quest for Digital Sovereignty », in *The Diplomat*, 19 mars 2025. https://thediplomat.com/2025/03/southeast-asias-quest-for-digital-sovereignty/. Consulté le 19 mai 2025.

nationale »[1217], déclarait ainsi en 2022 le ministre indonésien des Communications, alertant contre un « *colonialisme numérique »*[1218] qui reproduirait les schémas centre-périphérie du passé. En pratique, plusieurs ont adopté des lois de localisation des données. Le Vietnam exige depuis 2022 que Facebook, Google et consorts stockent les données utilisateurs localement[1219], et l'Indonésie impose depuis 2018 que les données gouvernementales soient hébergées sur le sol national [1220]. Singapour, quant à elle, se positionne comme un intermédiaire neutre en hébergeant des nœuds locaux de cloud internationaux tout en développant ses propres capacités [1221]. Si les normes se fragmentent par blocs, on peut imaginer les pays de l'ASEAN cherchant une troisième voie régionale, par exemple via un cadre commun de gouvernance des données au niveau ASEAN, et des bases ont été posées dans ce sens avec la fondation de l'ASEAN Data Management Framework. Cependant, la disparité d'intérêts entre des pays comme le Laos très dépendant de la Chine et le Vietnam méfiant envers Beijing, rendra difficile un front totalement uni. Certains choisiront l'alignement opportuniste sur le standard le plus avantageux économiquement, d'autres tenteront de jouer les blocs les uns contre les autres pour préserver leur marge de manœuvre.

L'Afrique, continent souvent pris en étau dans les rivalités de puissances, développe également un discours de souveraineté numérique. Beaucoup de gouvernements africains, séduits par l'offre « clé en main » de la Chine (infrastructures financées via les Nouvelles Routes de la Soie numériques, centres de données, surveillance, etc.), ont calqué des éléments du modèle chinois de gouvernance des données. Le Sénégal, par exemple, a inauguré en 2021 un data center national construit et financé par la Chine, en déclarant que cela permettrait de *« mieux contrôler son destin numérique et de résoudre définitivement la question de sa souveraineté digitale »*[1222]. Toutefois, cette dépendance envers la technologie chinoise comporte des risques. L'affaire d'espionnage entourant le siège de l'Union africaine, construit par la Chine à Addis-Abeba et qui exfiltrait clandestinement ses données vers Shanghai chaque nuit, en ayant été un exemple frappant [1223]. Ce type d'affaires a sensibilisé les pays

---

[1217] « Indonesia minister warns of digital colonialism as data law looms », Reuters, Jakarta, 21 juin 2022 [Johnny G. Plate, ministre indonésien des Communications et des Technologies de l'information].

[1218] Ibid.

[1219] Gunther Mackenzie, « Digital Sovereignty in ASEAN », PS-engage, 2024. https://ps-engage.com/digital-sovereignty-in-asea/. Consulté le 2 janvier 2025.

[1220] Xiriu Li, « Southeast Asia's Data Localization Push Is a Double-Edged Sword », in *The Diplomat*, 28 octobre 2022. https://thediplomat.com/2022/10/southeast-asias-data-localization-push-is-a-double-edged-sword/. Consulté le 12 mars 2025.

[1221] Singapour a ainsi lancé sa propre initiative sur le développement de l'IA dans le pays, dénommé « IA Singapour ». https://aisingapore.org/.

[1222] Folashadé Soulé, « Digital Sovereignty in Africa: Moving beyond Local Data Ownership », Center for International Governance Innovation, Policy Brief n°185, juin 2024, p.4. https://www.cigionline.org/static/documents/PB_no.185.pdf. Consulté le 21 janvier 2025.

[1223] Pilling D., Feng E., « African Union accuses China of hacking headquarters », *Financial Times*, 29 janvier 2018 ; « How China spied on the African Union for five years », Le Monde / AFP, 26 janvier 2018. Beijing a formellement démenti ces accusations.

africains à ne pas échanger une dépendance contre une autre. L'Union africaine a ainsi adopté, en 2020, une Stratégie africaine de transformation numérique, prônant un développement des infrastructures et compétences locales [1224]. En 2022, le Sommet de l'UA a renforcé ce cadre en validant notamment un Cadre de politique de données et un Cadre commun d'interopérabilité pour l'identité numérique. Ainsi, certains pays africains recherchent des solutions européennes alternatives aux offres chinoises, notamment en matière de protection des données ou de gouvernance d'Internet, afin de diversifier leurs partenariats. Néanmoins, la réalité économique pèse lourd, les équipements chinois restent moins coûteux et plus faciles d'accès, tandis que les plateformes américaines dominent l'usage quotidien. Dans un scénario de blocs, il est probable que l'Afrique deviendrait un terrain de concurrence normative acharnée où chaque bloc cherchera à y diffuser ses standards, notamment par le biais d'aides, de formations, d'investissements dans les universités et organismes de normalisation locaux. Les pays africains tenteront probablement quant à eux de maximiser leurs bénéfices en acceptant tantôt les normes de l'un, tantôt de l'autre, avec le risque d'une fragmentation interne au continent durable, si aucune coordination n'est menée au niveau de l'Union africaine.

À l'instar de l'ASEAN et de l'Afrique, l'Amérique latine oscille entre des liens historiques avec l'Occident et les nouvelles opportunités offertes par la Chine. Le Brésil, puissance régionale, a affiché des velléités de souveraineté numérique dès les années 2010 avec notamment la proposition de la présidente Dilma Rousseff d'un câble internet Brésil – Europe pour contourner les États-Unis suite aux révélations d'espionnage de la NSA en 2013 [1225]. Le Brésil et d'autres pays latino-américains participent au bloc des BRICS aux côtés de la Chine et de la Russie, où la question d'une coopération technologique indépendante de l'Occident est régulièrement soulevée. Par ailleurs, la région s'inspire souvent des réglementations européennes. Le Brésil a ainsi son LGPD sur les données personnelles inspirée du RGPD [1226]. En cas de fragmentation normative mondiale, les réponses des différents pays sud-américain pourraient être très variées d'un pays à l'autre. Ainsi, un pays comme le Venezuela sous sanction américaine sera plus proche du bloc sino-russe, tandis qu'un Chili ou une Colombie libérale resteront connectés aux États-Unis. Un défi majeur pour ces pays sera de ne pas subir une fragmentation interne où chaque changement de majorité politique amènerait un changement de

[1224] Union Africaine, « Stratégie de développement numérique pour l'Afrique », 2019. Disponible ici :https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_French.pdf. Consulté le 7 février 2026.

[1225] Classe Internationale, « Les câbles sous-marins au centre des enjeux de puissance mondiale : EllaLink, une alternative de gouvernance de l'Internet », 15 juin 2021. https://classe-internationale.com/2021/06/15/les-cables-sous-marins-au-centre-des-enjeux-de-puissance-mondiale-ellalink-une-alternative-de-gouvernance-de-linternet/. Consulté le 7 février 2026.

[1226] Protection des données, « LGPD vs RGPD: Analyse de la loi brésilienne sur la protection des données », 1er mars 2024. https://www.protection-des-donnees.fr/lgpd-letat-actuel-de-la-loi-bresilienne-sur-la-protection-des-donnees-personnelles/. Consulté le 7 février 2026.

fournisseurs et de normes technologiques, rendant les systèmes nationaux hétérogènes. Ainsi, le paysage global hors superpuissances est loin d'être passif. Beaucoup de pays articulent leur propre vision d'une souveraineté numérique maîtrisée, refusant l'hégémonie exclusive d'un modèle. Cependant, leur capacité réelle d'influence normative est limitée individuellement. L'UE apparaît parfois comme un allié potentiel de ces pays dans la défense d'un cyberespace ouvert et multipolaire, bien que son ancrage occidental limite sa portée auprès de certains. Ainsi, dans le scénario de fragmentation normative par blocs, on ne doit pas sous-estimer la capacité du Sud global à redéfinir partiellement les lignes de fracture.

L'analyse des domaines techniques susceptibles d'être fragmentés révèle que la normalisation géospatiale constitue donc un terrain privilégié de la compétition géopolitique contemporaine. Loin d'être de simples conventions techniques destinées à faciliter l'interopérabilité des systèmes, les formats de données, les référentiels géodésiques et les ontologies cartographiques incarnent des visions du monde, des représentations de l'espace et des rapports de pouvoir. Maîtriser les normes qui structurent l'information géographique, c'est contrôler les conditions de production, de circulation et d'interprétation des données territoriales. C'est pourquoi les grandes puissances investissent massivement dans le développement de standards propres et dans leur diffusion internationale. La fragmentation normative qui s'esquisse n'est pas un effet collatéral des tensions géopolitiques, elle en constitue l'un des fronts les plus stratégiques, car elle engage la capacité des États à représenter le monde selon leurs intérêts et à imposer cette représentation à leurs partenaires et rivaux. Si la fragmentation normative par blocs se réalise, elle ne touchera pas tous les aspects de l'écosystème géospatial avec la même intensité. Il est donc crucial d'identifier les domaines techniques où une divergence de standards entre blocs géopolitiques est la plus probable.

Ainsi, on peut distinguer plusieurs secteurs et technologies géographiques susceptibles d'être fragmentés et les formes que pourrait prendre cette fragmentation. Les formats de données et référentiels géodésiques constituent la base de toute infrastructure d'information géographique. Jusqu'à présent, une convergence relative existait autour de standards ouverts ou de facto : par exemple, le format Shapefile ou GeoJSON pour les données vecteurs, GeoTIFF pour les images, ou encore les référentiels globaux comme WGS84 pour les coordonnées GPS. Dans un scénario de blocs, des formats concurrents non interopérables favorisés par chaque bloc pourraient émerger. Dans cette situation, l'Occident continuerait à utiliser les normes de l'OGC et de l'ISO/TC 211, tandis que la Chine pourrait promouvoir des formats nationaux propriétaires ou dérivés. Ainsi, la Chine impose déjà sur son territoire l'utilisation de son système de coordonnées modifié (GCJ-02, souvent appelé « Mars Coordinates ») pour des raisons de sécurité. Les données géographiques publiquement accessibles en Chine sont décalées si elles ne sont pas converties via l'algorithme secret d'État, empêchant

l'utilisation directe de données GPS standard [1227]. Ceci est un exemple concret de fragmentation normative de jure. À l'avenir, la Chine pourrait étendre cette logique en exportant son référentiel géodésique et ses projections cartographiques via les projets qu'elle finance dans le monde, instaurant ainsi un écosystème parallèle de données géoréférencées. De même, la Russie pourrait renforcer l'adoption de son système PZ-90 qui sert de référentiel au système GLONASS, dans son aire d'influence [1228], au détriment du WGS84 américain. Ainsi, une fracture géopolitique globale des espaces normatifs pourrait avoir de lourdes conséquences sur la diffusion des données géographiques à l'échelle mondiale. En définitive, la fragmentation des formats de données et des référentiels géodésiques illustre parfaitement l'imbrication entre normalisation technique et rapports de puissance. Deux logiques géopolitiques se conjuguent dans ce domaine. La première est une logique de souveraineté défensive. En imposant des référentiels nationaux comme le GCJ-02 ou le PZ-90, les États protègent leurs données territoriales sensibles contre l'exploitation par des puissances étrangères. La deuxième est une logique d'influence offensive. En exportant leurs standards vers les pays partenaires, les grandes puissances créent des écosystèmes techniques qui verrouillent les dépendances à long terme. Ces logiques convergent vers une seule conclusion. Dans un monde fragmenté en blocs géopolitiques, il n'existerait plus de représentation commune de l'espace terrestre, même uniquement physique, mais des cartographies concurrentes reflétant les intérêts et les visions de chaque bloc.

[1227] Yongming Xu, Benjamin Lewis et Weihe Wendy Guan, « Developing the Chinese Academic Map Publishing Platform », in *Spatial Literary Studies in China*, Geocriticism and Spatial Literary Studies, Palgrave Macmillan, Cham, 2022, p 53 – 80. https://link.springer.com/chapter/10.1007/978-3-031-03914-0. Consulté le 23 janvier 2025.

[1228] Demianov G.V., Kaftan V.I., Makarenko N.L., Zabnev V.I., Zoubinski V.I., « New Russian Reference Frame: Status and Development », in *National Reports*, 2000, pp. 293 – 300. https://d1wqtxts1xzle7.cloudfront.net/47879547/New_Russian_Reference_Frame_Status_and_D20160808-30010-y9xmld-libre.pdf. Consulté le 23 janvier 2025.

1.2 Une fracture normative internationale menacerait l'échange d'informations à l'échelle mondiale

Les API et protocoles de services géospatiaux sont un autre champ de possible fragmentation. Actuellement, les applications géospatiales globales s'appuient sur des protocoles standardisés, tels que WMS/WFS pour la diffusion de cartes et de données, ou plus récemment les API REST OGC (OGC Features API, etc.). Dans un monde fragmenté, il pourrait être envisageable que ces standards ouverts cessent d'être universellement adoptés. Il en résulterait que d'un côté, le bloc occidental continuerait à faire évoluer les API OGC en misant sur l'ouverture et l'interopérabilité, tandis que de l'autre la Chine, si elle se sent marginalisée dans ces organismes, pourrait promouvoir des interfaces propriétaires pour ses plateformes, à l'image de Baidu Maps API, Gaode Maps API, qui ne correspondent pas exactement aux standards OGC, mais dominent le marché chinois. À terme, des écosystèmes d'API incompatibles pourraient se développer en parallèle. Dans un tel cas de figure, une application développée pour consommer des données via les services Web occidentaux (ex. l'API Google Maps, ou un flux WFS standard) ne pourrait pas aisément se connecter aux services équivalents dans l'environnement chinois, et vice versa. Certes, des passerelles pourraient exister, par exemple des serveurs de conversion, mais elles ajouteraient de la complexité et de la latence. Si aujourd'hui le protocole NMEA pour les signaux GNSS est universel, demain, chaque bloc pourrait chiffrer ou signer différemment ses données de position, rendant plus difficile la conception d'un récepteur universel. Dans le même ordre d'idée, les standards de communication machine – to – machine pourraient diverger. Ainsi, les échanges de données géographiques pourraient devenir beaucoup plus laborieux en cas de fragmentation normative des technologies liées aux données géographiques, nécessitant un nombre important d'adaptateurs intermédiaires pour faire circuler des données partout dans le monde.

L'IA géospatiale, est également un domaine très sensible aux normes, notamment en ce qui concerne les jeux de données d'entraînement. Une telle fragmentation pourrait d'abord affecter les formats de données utilisés pour l'entraînement des modèles d'intelligence artificielle. Les corpus de données géospatiales, essentiels au bon fonctionnement des algorithmes, risqueraient d'être structurés différemment selon les zones d'influence. Par exemple, dans les pays occidentaux, les formats tels que TFRecord, associé à l'écosystème TensorFlow[1229], de plus en plus adopté comme standard, sont largement utilisés. À l'inverse, la Chine pourrait promouvoir ses propres formats optimisés pour des frameworks domestiques, à l'instar de PaddlePaddle[1230], son environnement d'IA national. Cette

[1229] TensorFlow est un outil open source d'apprentissage automatique développé par Google. Voir : Release TensorFlow 2.20.0 · tensorflow/tensorflow.

[1230] PaddlePaddle est le pendant chinois de TensorFlow, ouvert à tous en 2016. Le Github du projet est accessible en ligne: PaddlePaddle

incompatibilité dans les formats d'encodage rendrait difficile, voire impossible, le partage fluide de jeux de données d'entraînement entre ces différentes sphères technologiques. La fragmentation par bloc s'est également étendue à l'architecture logicielle des outils d'intelligence artificielle. Si les frameworks occidentaux, comme TensorFlow continuent à dominer en Europe et en Amérique du Nord, d'autres environnements, comme PaddlePaddle s'imposent en Chine avec des évolutions propres, non nécessairement compatibles. Cette divergence pourrait engendrer une scission durable entre les écosystèmes logiciels, rendant le transfert d'un algorithme d'un environnement à l'autre particulièrement complexe. En résumé, l'IA géospatiale, au lieu d'être un vecteur d'analyse universel du globe, risque d'être compartimentée. À terme, chaque bloc accumulerait potentiellement un retard sur certains cas d'usage non développé chez lui faute d'accès aux données. Ainsi, un bloc qui n'a pas accès aux données contrôlées par un autre via ses satellites ne peut pas développer d'IA performante dans ce domaine. Cela soulève des enjeux de dépendance scientifique et de distorsion dans la maîtrise de l'information géographique mondiale.

La cybersécurité appliquée aux systèmes géospatiaux est un autre domaine où la fragmentation normative est une réalité, notamment du fait de l'arrivée de la cryptographie post-quantique et de la menace quantique sur les infrastructures existantes. Les normes de sécurité déterminent comment les données et communications géospatiales sont protégées. Si chaque bloc adopte ses propres standards de chiffrement, de protocoles réseau sécurisés et de résilience quantique, on fera face à des systèmes cloisonnés par des murs cryptographiques. Ainsi, si aujourd'hui, la plupart des acteurs utilisent le protocole TLS/SSL pour sécuriser les échanges Web, y compris les services cartographiques en ligne, avec l'arrivée des ordinateurs quantiques, ces algorithmes devront être remplacés par des alternatives post-quantiques. Comme souligné plus haut, si les États-Unis, via le NIST, ont pris les devants en standardisant en 2022-2024 quelques algorithmes PQC. Cependant, rien ne garantit que la Chine ou la Russie adopteront ces choix. Concrètement, cela pourrait signifier qu'à terme les systèmes sécurisés d'un bloc ne reconnaîtront pas comme sûres les communications de l'autre bloc. Si une telle situation venait à se produire, un flux de données géospatiales chiffré avec un algorithme post-quantique américain pourrait être bloqué par les pare-feux chinois qui n'en connaissent pas la méthode, et inversement, une télétransmission sécurisée par QKD chinois ne serait pas intégrable dans les réseaux occidentaux non équipés de ces technologies.

Ainsi, le principal enjeu de ce scénario de fragmentation normative est sans conteste l'interopérabilité, ou plutôt la perte d'interopérabilité, entre les systèmes géospatiaux à l'échelle mondiale. L'interopérabilité est le fruit de décennies de standardisation. Or, une fragmentation par blocs signifierait un coup d'arrêt à cette dynamique, avec un risque de fracture du Web géospatial en plusieurs réseaux partiellement isolés. Cela pourrait aboutir à un véritable splinternet étendu au

domaine géospatial tout entier. Des infrastructures de données spatiales régionales seraient développés par chaque bloc, mais avec des passerelles limitées entre elles. Ainsi, une Infrastructure de Données spatiales paneuropéenne qui serait bâtie sur INSPIRE et les normes OGC, coexisterait avec une infrastructure eurasienne exploitée par la Chine, la Russie et leurs alliés, avec leurs propres catalogues et formats. Les deux contiendraient des données globales, mais dans des formes différentes. Pour un acteur souhaitant avoir une vision vraiment mondiale, il faudrait presque maintenir deux systèmes en parallèle et assurer soi-même la conversion, ce qui n'est envisageable que pour de très grosses structures. Les plus petits acteurs, comme les PME, ou les universités risqueraient de se retrouver enfermés dans l'un des écosystèmes, perdant l'accès à une partie du savoir ou des services géospatiaux disponibles ailleurs. L'absence de normes communes signifierait que les mêmes fonctions devraient être redéveloppées selon différents standards. Par exemple, un fabricant de GPS devrait intégrer 4 ou 5 modules au lieu d'un seul : un pour chaque système de navigation (GPS, Galileo, BeiDou, GLONASS) avec leur protocole spécifique et cryptographie associée. De même, un développeur d'application de cartographie pourrait devoir coder ses appels de services pour Google, pour Baidu, pour OpenStreetMap, etc., séparément. Cette duplication d'efforts représente un immense gaspillage économique à l'échelle mondiale. Elle pourrait freiner l'innovation, car l'énergie dépensée à adapter/convertir n'est pas dépensée à améliorer. En cas de rupture normative globale, les marchés se fragmenteraient. Des fournisseurs de données ou de logiciels auraient accès à un bloc, mais pas aux autres, limitant leurs économies d'échelle. Pour les consommateurs finaux, le choix serait plus restreint au sein de chaque bloc, donc potentiellement plus coûteux faute de concurrence mondiale. Si aujourd'hui, malgré les tensions, la communauté internationale peut s'appuyer sur des données et systèmes globalement compatibles, dans un monde fragmenté, ces synergies seraient plus difficiles. La coopération scientifique pourrait s'en trouver également ralenti. Par exemple, en cas de catastrophe naturelle majeure affectant plusieurs pays de blocs différents, le partage en temps réel d'images de drones ou de cartes d'impact, pourrait être retardé si chaque équipe utilisait des formats et réseaux différents, nécessitant des conversions d'urgence susceptibles d'entraîner des erreurs.

Il faut également noter que la fragmentation normative poserait à la France un défi important. En tant que membre de l'UE, la France s'inscrirait sans doute dans le bloc occidental, adoptant ses normes. Elle bénéficierait donc de l'interopérabilité interne de ce bloc, mais subirait les limitations vis-à-vis des autres blocs. Pour ses besoins nationaux, la France devrait probablement doubler certains outils pour pouvoir continuer à interagir avec les zones hors bloc, notamment pour maintenir des capacités d'accès aux systèmes chinois ou russes pour le renseignement géographique, tout en se sécurisant contre eux. Cela représente bien évidemment un coût et une complexité accrus pour les institutions nationales. Toutefois, cela pourrait consister également en une opportunité. La France, via

l'UE, pourrait jouer un rôle de médiateur technique entre les normes, forte de sa présence historique dans les instances de normalisation internationales. À condition d'investir suffisamment, la France pourrait contribuer à ces fameux standards passerelles, ou promouvoir une approche open source inclusive qui atténue la fragmentation. Cependant, globalement, la fragmentation affaiblirait la position française si elle devait se priver de l'apport de tout un pan de l'innovation mondiale situé hors de son bloc, d'où l'enjeu pour elle de soutenir les efforts internationaux cherchant à éviter la fermeture totale du cyberespace géographique.

1.3 Vers une guerre froide normative sans vainqueur ?

Au-delà des aspects techniques, la fragmentation normative par blocs traduit et amplifie des dynamiques géopolitiques profondes. C'est à la fois un reflet des rapports de puissance du moment et un facteur de recomposition de ces rapports. La fragmentation pourrait paradoxalement accroître certaines dépendances au lieu de les réduire. En effet, si un pays choisit un camp technologique, il devient tributaire de ce camp pour les évolutions futures. Autrement dit, la fragmentation normative peut cimenter des zones d'influence en verrouillant les pays dedans. Cela s'observe déjà chez les pays fortement équipés par la Chine en télécoms, il leur est structurellement difficile de changer de fournisseur, car tout leur réseau est calibré sur Huawei et serait incompatible avec, par exemple, du Cisco sans refonte totale.

De même, les grandes puissances elles-mêmes ne sont pas totalement indépendantes, même dans un monde fragmenté. Ainsi, même les États-Unis continueraient à dépendre de la Chine pour certaines terres rares et composants, tandis que la Chine dépend de l'Occident pour certains logiciels ou microprocesseurs, du moins tant qu'elle n'a pas tout substitué localement, ce qui est en cours, mais pas terminé. La fragmentation normative ne supprime pas ces dépendances structurelles de la chaîne d'approvisionnement, elle les recompose en blocs plus étanches. Chaque bloc tenterait de minimiser ses dépendances externes. Par exemple, l'Europe parle d'« autonomie stratégique » et investit pour produire ses propres satellites, ses propres solutions cloud, etc., et la Chine également. Mais il est impossible pour un bloc d'exceller en tout, et par conséquent des points faibles subsisteront. Qui dit fragmentation dit aussi moins de diversité de fournisseurs par bloc, donc potentiellement plus de vulnérabilité aux défaillances internes. Si, par exemple, le bloc occidental ne compte plus qu'un ou deux grands acteurs pour un type de donnée critique, une panne ou une attaque sur eux pourrait priver tout le bloc de ce service, sans recours à un fournisseur alternatif étranger. La résilience globale des systèmes pourrait donc baisser. La constitution de blocs normatifs n'épousera pas nécessairement

exactement les alliances politiques existantes, elle peut aussi les bousculer. Des pays traditionnellement alliés pourraient diverger s'ils font des choix technologiques opposés. À l'extrême, cela pourrait créer de nouvelles lignes de fracture géopolitiques inattendues. Par exemple, imaginons que certains pays européens, lassés de dépendre du duopole américano-chinois, décident de s'allier pour adopter un troisième ensemble de normes indépendantes, s'ils persistent dans cette voie au point de refuser aussi bien les solutions US que chinoises, cela pourrait les éloigner stratégiquement des États-Unis, créant une tension au sein de l'Alliance occidentale, mais qui pourrait constituer par la même occasion une voie pour sauvegarder les intérêts européens. Ainsi, la fragmentation normative pourrait obliger à redéfinir certaines alliances en fonction des orientations techno-industrielles de chacun.

Inversement, des pays jusqu'ici peu alignés pourraient se rapprocher grâce à un choix normatif commun. Par exemple, si l'Arabie Saoudite adopte massivement des technologies chinoises, ce qu'on observe déjà dans certaines Smart Cities du Golfe [1231], elle pourrait se retrouver beaucoup plus liée à la Chine sur le plan militaire et stratégique, ce qui la ferait basculer géopolitiquement vers le bloc sino-russe, alors même qu'historiquement, elle se situe dans l'orbite américaine. Au final, la carte du monde des alliances pourrait être redessinée en fonction de critères technico-normatifs autant que politico-idéologiques.

Pour certains États, la possibilité d'un isolement normatif presque total semble une possibilité envisageable, voire même souhaitable jusqu'à un certain point (Russie et Chine en tête). Cependant, une telle politique présenterait un coût extrêmement élevé en freinant l'innovation, et provoquerait un cloisonnement important. Ainsi, pour la France et d'autres pays européens, la souveraineté numérique ne peut s'envisager hors d'un cadre coopératif, notamment celui de l'UE et dans l'ouverture, ce qui milite contre une fragmentation excessive. En dehors de cette vision européenne plutôt axée sur l'ouverture, la souveraineté numérique est souvent synonyme de contrôle national sur les données et les infrastructures. Beaucoup de pays se sont mis à localiser les données sur leur territoire, ou encore à construire des fermes de serveurs locaux, le tout afin de sortir du régime antérieur désormais jugé inadmissible où la totalité des infrastructures étaient hébergées aux États-Unis. Si ces politiques renforcent la souveraineté des États, elles réduisent du même coup l'interopérabilité mondiale si des normes communes ne sont pas adoptées afin de permettre à l'ensemble des données de continuer à circuler entre ces différents blocs. La liberté absolue dans le cyberespace reste une chimère pour la majorité des pays, et n'est peut-être possible que pour les grandes puissances qui peuvent développer un écosystème complet chez eux. Pour les autres, la souveraineté passe paradoxalement par la coopération, et l'Europe présente ici un des meilleurs cas de figure d'une coopération transnationale

[1231] George Rachel, « The Rise of Gulf Smart Cities », Wilson Center, 16 septembre 2024. https://www.wilsoncenter.org/article/rise-gulf-smart-cities. Consulté le 4 avril 2025.

qui participe à renforcer la souveraineté de tous les États membres. D'autres organisations, comme l'Union africaine cherchent également à remplir ce rôle, bien que de façon bien moins efficace pour le moment. En cas de fragmentation normative par blocs, des pôles de souveraineté collective pourraient être amenés à émerger. Ces pôles pourraient se substituer aux États-nations comme unités pertinentes du débat normatif. Dans un monde en blocs, la souveraineté nationale prendra la forme d'une souveraineté de bloc où chaque bloc aura sa « citadelle numérique » où il fait respecter ses lois, et les nations à l'intérieur auront une marge de manœuvre limitée vis-à-vis des normes du bloc dominant. Ainsi, si un scénario de fragmentation normative global venait à se confirmer, seules les grandes puissances pourraient y voir un quelconque bénéfice, car elles pourraient maintenir leur domination en cadenassant leur zone. Les grands perdants de ce phénomène seraient de loin les espaces aujourd'hui non alignés, qui risqueraient de devenir des champs de bataille normatifs sans avoir voix au chapitre, ou qui devront se soumettre à l'un ou l'autre.

La normalisation internationale n'échappe donc pas à une tendance en réalité plus large, qui est la fragmentation géoéconomique globale. Dès juin 2022, le conseiller économique du FMI Pierre-Olivier Gourinchas mettait en garde contre le risque d'une fracturation du monde en *« blocs économiques distincts avec des disparités d'idéologies, de systèmes politiques, de normes technologiques, de systèmes de paiement et de commerce transfrontaliers »*[1232]. Cette analyse s'applique directement au domaine normatif géospatial. En effet, une fragmentation des standards techniques en blocs étanches reproduirait à l'échelle des infrastructures numériques les mêmes dynamiques de découplage qui menacent les chaînes d'approvisionnement mondiales [1233]. Ce découplage pourrait se renforcer de lui-même, en effet, plus les normes divergent, plus les échanges diminuent, et plus chaque bloc se replierait économiquement sur son groupe. C'est un cercle potentiellement vicieux menant à un monde bipolaire ou tripolaire consolidé. La compétition pour rallier les pays tiers ferait rage, y compris via des incitations normatives (par exemple, offrir l'accès libre à un ensemble de données globales pour inciter à rejoindre tel bloc standard). Au final, la normalisation technique n'est jamais « neutre », elle sert les intérêts de celui qui l'impose. Ici, chaque bloc voudra gagner cette course pour ne pas être celui qui doit plier devant le standard de l'autre.

Ainsi, une fragmentation normative par blocs géopolitiques entraînerait un futur dans lequel le cyberespace géographique se morcelle, reflétant et renforçant les divisions entre puissances. Des lignes de fracture actuelles, rivalité sino-américaine, quête d'autonomie russe, volontarisme réglementaire européen, assertivité des puissances émergentes, pourraient aboutir à un monde où plusieurs

[1232] Gourinchas Pierre-Olivier, « Un casse-tête géoéconomique », *Finances & Développement*, Fonds monétaire international, Washington D.C., juin 2022, pp. 4–7.

[1233] Shekhar Aiyar, Jiaqian Chen, Christian Ebeke et al., « Geoeconomic Fragmentation and the Future of Multilateralism », International Monetary Fund, Staff Discussion Note, janvier 2023, p. 10.

écosystèmes technologiques géospatiaux coexistent sans bien communiquer entre eux. Les domaines clés, comme les formats de données, les protocoles, l'IA, la sécurité ou les métavers deviendraient des champs de compétition normative, au risque de briser l'interopérabilité mondiale. Les conséquences toucheraient aussi bien à l'efficacité économique qu'à la capacité à relever des défis planétaires (climat, gestion de crise), et entraînerait inévitablement une érosion de la souveraineté des États, en accentuant la dépendance envers les pays majeurs de ces nouveaux blocs de puissance. Face à cette perspective, des stratégies diverses se dessinent, entre alignement complet sur une grande puissance pour bénéficier de son giron technologique, ou au contraire non-alignement et recherche d'alternatives pour éviter une nouvelle sujétion numérique. La réalité verra sans doute des positionnements nuancés et évolutifs, chaque État ou région tentant de maximiser ses avantages. Géographiquement, cela aboutirait à la constitution de sphères d'influence numériques rappelant la Guerre Froide, mais avec la complexité supplémentaire d'une interconnexion minimale qu'il faudra préserver pour ne pas tomber dans un chaos numérique total. En définitive, du point de vue de la souveraineté nationale française, ce scénario de fragmentation serait à craindre. La France, au sein de l'UE, aurait intérêt à privilégier la coopération internationale sur les normes pour éviter de se retrouver enfermée dans un schéma binaire restrictif. Tout en renforçant sa capacité à évoluer dans un environnement multipolaire, elle gagnerait à soutenir les efforts de standardisation ouverte et inclusive qui peuvent prévenir l'avènement d'un cyberespace aussi fragmenté. En conclusion, se dessine ici un enjeu central. La bataille des normes géographiques est aussi une bataille pour la gouvernance du numérique mondial. Selon que l'issue penche vers la fragmentation ou vers l'harmonisation, les équilibres de puissance et la nature même de la souveraineté numérique au XXIe siècle pourraient être très différents.

2. Stratégies d'influence pour les acteurs publics et privés

2.1. Diplomatie normative et soft power des États

Le cyberespace et les données numériques sont devenus des terrains diplomatiques où se joue un jeu d'influence normatif. La diplomatie normative consiste à promouvoir par la persuasion et la coopération internationale un jeu de règles et de standards préférés. Cette diplomatie technique s'appuie sur le concept de soft power. En façonnant les normes du numérique (interopérabilité, sécurité, protection des données, etc.), les États cherchent à ancrer leurs valeurs et intérêts dans la gouvernance mondiale. Comme le notent certains experts, *« dans la cybersécurité et les télécoms, le jeu des grandes puissances n'est pas seulement un jeu de technologie, mais aussi d'idées et de pouvoir de discours »*[1234]. Autrement dit, maîtriser les processus normatifs (standards, protocoles, régulations) est un levier majeur de puissance douce pour les puissances globales. Chaque grande puissance a élaboré une doctrine ou stratégie nationale de diplomatie numérique, avec ses priorités stratégiques. En France et dans l'UE, la Stratégie internationale de la France pour le numérique insiste sur l'Internet ouvert, la cybersécurité, les droits de l'homme et l'influence technologique [1235]. Quatre enjeux y sont identifiés : la sécurité du cyberespace, la gouvernance ouverte d'Internet, la promotion des valeurs démocratiques et l'attractivité des acteurs français du numérique [1236]. L'ambassadeur français pour le numérique doit coordonner l'élaboration de ces positions à l'international et les promouvoir auprès des partenaires. À l'échelle européenne, la diplomatie numérique de l'UE vise à « *garantir le rôle mondial de l'UE dans le monde digital, protéger ses intérêts stratégiques et promouvoir son cadre réglementaire humain et inclusif »*[1237], notamment via le Digital Single Market et le RGPD. Les conclusions du Conseil UE 2022-2023 appellent à une approche « Team Europe » renforcée.

Quant à elle, l'administration américaine a réaffirmé les idéaux d'un Internet « libre, sécurisé, interopérable et fiable », tout en renforçant ses alliances numériques. En 2022, le département d'État a créé le Bureau du cyberespace et de la politique numérique (CDP), dirigé par un Ambassadeur itinérant pour le cyberespace et la politique numérique, pour promouvoir un *« comportement responsable des États dans le cyberespace »* et l'*« Internet ouvert »*[1238]. La nouvelle Stratégie internationale 2024 du

---

[1234] Doshi Rush, de La Bruyère Emily, Picarsic Nathan et Ferguson John, « China as a « Cyber Great Power » : Beijing's two voices in communications », Foreign Policy, Security, strategy and order, BOOKINGS, avril 2021, p.10.

[1235] Ministère de l'Europe et des Affaires étrangères, « Stratégie internationale de la France pour le numérique », 2020, p. 4. https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.

[1236] https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/

[1237] Conseil de l'Union européenne, « Conclusions du Conseil sur la diplomatie numérique de l'UE », 10526/23, 26 juin 2023, p.3.

[1238] US Department of State, « United States International Cyberspace & Digital Policy Strategy : Towards an Innovative, Secure, and Rights-Respecting Digital Future », 6 mai 2024. https://www.state.gov/united-states-international-

Cyberspace promeut la *« solidarité numérique »* pour bâtir un écosystème ouvert, résilient, défendable et respectueux des droits. Les États-Unis mènent ainsi un agenda multilatéral axé sur la coopération avec les alliés (par ex. le Conseil Commerce-Technologie UE-US) et la défense des normes fondatrices du Web global, tout en sanctionnant (via contrôles technologiques ou embargos) les acteurs jugés contraires à leurs intérêts.

Au même moment, Beijing avance un modèle de « souveraineté cybernétique » affirmée. La Chine entend gagner en influence dans les instances normatives internationales. Selon une étude, sa stratégie China Standards 2035 lancé fin 2021, a fixé pour objectif d'augmenter *« le nombre de normes internationales chinoises et de représentants chinois dans les postes de direction »*[1239] au sein des organismes de normalisation. Officiellement, elle prône le multilatéralisme intergouvernemental (via l'UIT), tandis qu'en interne, elle « dilue » ce discours en insistant sur le caractère coopératif de ses propositions. Cependant, les revues chinoises affirment aussi la « valeur concurrentielle des normes » pour asseoir la domination technologique, rappelant que *« celui qui définit les normes dirige le monde »*[1240]. Par ailleurs, la Chine projette sa diplomatie normative à travers l'initiative des Nouvelles Routes de la Soie numériques amorcée en 2015, qui s'accompagne systématiquement d'une diffusion de ses standards auprès des nations qui adhèrent au programme[1241].

Sur la scène internationale, les forums de normalisation et organismes internationaux de standardisation constituent toujours les principales instances où se joue l'avenir de la diffusion des avancées technologiques. Les gouvernements participent activement aux instances techniques, comme l'ISO, l'UIT, l'IETF, l'OGC ou l'ONU-GGIM. Ils y envoient des experts, financent des projets, et préconisent des standards. Il faut aussi prendre en compte que des coalitions ad hoc forment des blocs normatifs. À titre d'exemple, le Trade and Technology Council entre l'UE et les États-Unis a été créé pour aligner les positions des États membres sur les technologies sensibles et coécrire des normes. Le Quad (USA, Japon, Inde, Australie) définit des principes pour un Internet ouvert en Indo-Pacifique. Les États-Unis ont également lancé le Digital Connectivity and Cybersecurity Partnership (DCCP) en juillet 2018 pour promouvoir des infrastructures numériques « ouvertes, fiables et sécurisées » en Asie-

cyberspace-and-digital-policy-strategy/. Consulté le 12 juillet 2024.

[1239] Neaher Giulia, Bray David A., Mueller-Kaler Julian et Schatz Benjamin, « Standardizing the Future : How can the United States Navigate the Geopolitics of International Technology Standards? », Atlantic Council, Geotech Center, 14 octobre 2021, p. 16

[1240] Qiushi Magazine, « Xi Jinping : s'efforcer de devenir un centre scientifique et un centre d'innovation majeur dans le monde » (习近平称努力让关键核心技术自主可控促产业迈向全球价值链中高端), 15 mars 2021, https://www.gov.cn/xinwen/2021-03/15/content_5593022.htm. Consulté le 21 mars 2023

[1241] He Alex, « The Digital Silk Road and China's Influence on Standard Setting », CIGI Papers No. 264, avril 2022, p.3. https://www.cigionline.org/static/documents/no.264.pdf. Consulté le 2 janvier 2024.

Pacifique [1242]. Ces coalitions permettent de rédiger des normes communes ou de mutualiser les meilleures pratiques, créant ainsi des alternatives aux modèles chinois ou russes.

De plus, de plus en plus, une forme de diplomatie normative se développe. Les ambassadeurs et attachés spécialisés participent également à la diffusion de normes. Plusieurs pays ont nommé des représentants dédiés au numérique. Ainsi, la France dispose d'un Ambassadeur pour le numérique (poste instauré en 2017) qui coordonne les positions françaises en cybersécurité et gouvernance de l'Internet, et les promeut au sein des organisations internationales [1243]. Les États-Unis ont nommé en 2022 un Ambassadeur-at-Large for Cyberspace and Digital Policy dirigeant le Bureau CDP. D'autres pays comme la Grande-Bretagne, l'Allemagne, le Japon ou encore la Corée créent des postes d'attachés numériques ou d'ambassadeurs chargés du numérique. Ces diplomates techniques travaillent dans les ambassades et délégations permanentes pour participer aux débats sur la cybersécurité, la protection des données, l'intelligence artificielle, etc., les diplomates numériques s'appuient aussi sur la recherche et les programmes de développement industriel. Des programmes bilatéraux incluent des volets sur l'innovation digitale et la normalisation. Les missions scientifiques dans les pays partenaires favorisent l'appropriation des normes occidentales. En multilatéral, la diplomatie académique organise des forums thématiques comme Géoweb, ou Data Science, où États et industriels négocient les futures normes. Enfin, l'influence normative se diffuse également via la communication. La France et l'UE mettent en avant leur modèle de « numérique ouvert et sûr » dans les dialogues internationaux comme le Forum sur la gouvernance d'Internet, les Sommets numériques, et des initiatives de l'UNESCO, tandis que la Chine organise des événements d'affaires comme la China Standards Week, pour promouvoir ses normes. Les ambassades publient également sur les réseaux sociaux leurs positions normatives, cherchant à rallier l'opinion mondiale à leur vision.

L'influence normative dans le domaine géospatial et numérique obéit donc à une géographie profondément inégale qui reflète, tout en les renforçant, les structures de pouvoir globales. Cette géographie se caractérise par une concentration historique des capacités normatives dans les pôles technologiques occidentaux, une contestation croissante de cette hégémonie par la Chine, et l'émergence de stratégies différenciées parmi les puissances intermédiaires et les pays du Sud.

Les États-Unis et l'Europe ont historiquement dominé l'écosystème normatif international. Cette domination s'explique par trois facteurs convergents. Tout d'abord, la concentration des capacités d'innovation dans des pôles technologiques tels que la Silicon Valley ou les clusters européens, la taille

[1242] Digital Development, « USAID Digital Connectivity and Cybersecurity Partnership (DCCP) Factsheet », 2018. https://www.digitaldevelopment.org/library/usaid-digital-connectivity-and-cybersecurity-partnership-dccp-factsheet/.

[1243] Ministère de l'Europe et des Affaires étrangères, « Ambassadeur pour le numérique : Synthèse du rapport d'activité 2020 », 2020. https://www.diplomatie.gouv.fr/IMG/pdf/synthese_fr_rapport_d_activite_ambassadeur_pour_le_numerique_2020_cle068aba.pdf

des marchés intérieurs qui confère aux normes domestiques une portée mondiale par effet de masse critique, et l'ancienneté de la participation aux organismes de standardisation qui assure une surreprésentation dans les comités techniques et les postes de responsabilité[1244]. Les formats de données géospatiales de l'OGC, les protocoles Internet de l'IETF, les normes de sécurité du NIST constituent autant de standards d'origine occidentale devenus références mondiales de facto.

Cette hégémonie normative occidentale fait désormais l'objet d'une contestation systématique de la part de la Chine. Beijing a identifié la normalisation comme un levier stratégique de premier plan et déploie une stratégie cohérente articulant plusieurs dimensions. Sur le plan doctrinal, le programme China Standards 2035, lancé officiellement en 2018 dans le prolongement du plan Made in China 2025, fixe explicitement l'objectif de transformer les normes chinoises en normes globales, en particulier dans les domaines de l'intelligence artificielle, des réseaux de nouvelle génération et des données [1245]. Sur le plan institutionnel, la Chine a massivement investi sa présence dans les organismes internationaux, privilégiant l'Union internationale des télécommunications où le principe « un État, une voix » lui est plus favorable que la gouvernance multipartite de l'IETF ou de l'OGC [1246]. Sur le plan opérationnel, la Belt and Road Initiative numérique, annoncée en 2015 sous le nom de Digital Silk Road, conditionne les investissements dans les infrastructures digitales à l'adoption des standards technologiques chinois par les pays bénéficiaires[1247].

Cette contestation sino-américaine ne se réduit pas à une simple rivalité bilatérale. En effet, elle structure un clivage plus profond sur la conception même de la gouvernance numérique. D'un côté, les démocraties occidentales promeuvent un modèle de gouvernance multipartite associant États, entreprises, société civile et communauté technique, fondé sur des principes d'ouverture, d'interopérabilité et de protection des droits fondamentaux. De l'autre, la Chine et la Russie défendent une gouvernance intergouvernementale où la souveraineté étatique prime sur les autres considérations, légitimant le contrôle des flux de données au nom de la sécurité nationale [1248]. Ces deux visions s'affrontent dans toutes les enceintes internationales, engendrant ce que le Haut Représentant de l'Union

---

[1244] Tim Rühlig, Technical Standardization, China, and the Future International Order, Brussels, Heinrich Böll Foundation, 2022, p. 12-15.

[1245] Central Committee of the Communist Party of China and the State Council, « Outline for the development of national standardization », Xinhua, 10 octobre 2021

[1246] Borodyna Olena, « Russia's recent ITU election loss is a major setback for China's internet governance ambitions », ODI, 5 octobre 2022.

[1247] Fédération de Russie et République populaire de Chine, « Joint Statement of the Russian Federation and The People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Developement », Beijing, 4 février 2022, partie III. http://en.kremlin.ru/supplement/5770

[1248] Borodyna Olena, « Russia's recent ITU election loss is a major setback for China's internet governance ambitions », ODI, 5 octobre 2022

européenne Josep Borrell a qualifié, dans son discours de Bruxelles d'octobre 2022, de *« monde multipolaire désordonné »* caractérisé par une paralysie croissante des instances multilatérales [1249].

Dans ce contexte de bipolarisation, l'Union européenne occupe une position singulière, mais précaire. Singulière, car l'Europe tente aujourd'hui de définir une troisième voie normative fondée sur la régulation des acteurs dominants, la protection des données personnelles et l'affirmation d'une souveraineté numérique distincte de l'hégémonie américaine comme du modèle autoritaire chinois. Le RGPD constitue une parfaite illustration de cette « puissance normative européenne ». Adopté en 2016 et entré en vigueur en 2018, il a inspiré des législations similaires au Japon, au Brésil, en Corée du Sud, en Inde et dans plusieurs États américains, manifestant ce qu'Anu Bradford a théorisé sous le nom d'« effet Bruxelles »[1250]. Le Cyber Act, le Data Act, l'AI Act et l'initiative Global Gateway prolongent cette stratégie d'exportation normative vers les pays partenaires. Cette position reste précaire cependant, car cette ambition européenne repose sur un paradoxe : comment maintenir un leadership dans la définition des standards alors que le continent a perdu sa prééminence industrielle dans les technologies numériques ? De fait, l'Europe produit des normes, mais dépend largement des plateformes américaines et des équipements asiatiques pour les mettre en œuvre. Cette dissonance entre puissance normative et puissance industrielle constitue la principale vulnérabilité de la stratégie européenne. Les puissances émergentes et les pays du Sud global se trouvent quant à eux confrontés à un choix d'alignement normatif aux implications durables.

Les alliances régionales, qu'il s'agisse du partenariat transpacifique, du Quad indo-pacifique ou des initiatives de l'Union africaine, tentent de négocier des marges d'autonomie et une répartition plus équitable du pouvoir normatif. Toutefois, en l'absence de capacités propres de production de standards, ces acteurs demeurent structurellement dépendants. Ils se retrouvent obligés à choisir entre l'écosystème occidental et l'écosystème chinois, mais ils peuvent difficilement construire une alternative. Cette dépendance normative prolonge et approfondit les asymétries économiques et technologiques héritées de la mondialisation.

La diplomatie normative s'affirme ainsi comme une composante essentielle des stratégies de puissance contemporaines. Chaque État qui en possède les moyens articule désormais ses conceptions géopolitiques à un discours et une pratique normative visant à étendre son système de valeurs et de standards au-delà de ses frontières. Pour les grandes puissances, la normalisation constitue un instrument de projection d'influence, pour les puissances moyennes, un levier de différenciation stratégique, et pour les pays en développement, un terrain de négociation où se joue leur autonomie

[1249] Borrell Josep, « EU Ambassadors Annual Conference 2022: Opening Speech by High Representative Josep Borell », Bruxelles 10 octobre 2022. Texte disponible sur : https://www.eeas.europa.eu/eeas/eu-ambassadors-annual-conference-2022-opening-speech-high-representative-josep-borrell_en consulté le 10 mars 2025.

[1250] Bradford Anu, The Brussels Effect : How the European Union Rules the World, Oxford university Press, 2020.

future. Cette politisation croissante de la normalisation technique transforme les arènes de standardisation en espaces de confrontation géopolitique, où les enjeux de souveraineté numérique se superposent aux considérations d'interopérabilité et d'efficacité technique. Toutefois, dans le domaine de la production de normes, les États ne sont pas seuls. En effet, les consortiums privés de production et de diffusion de normes déploient également leurs propres stratégies pour faire adopter les standards désirés par leurs contributeurs.

2.2. Innovations stratégiques des consortiums privés

Les consortiums industriels jouent aujourd'hui un rôle central dans la définition des normes technologiques du cyberespace, opérant désormais comme des acteurs géopolitiques à part entière. Face aux menaces croissantes sur la cybersécurité et aux enjeux de souveraineté numérique, des observateurs soulignent que *« la normalisation des TIC deviendra le prochain champ de bataille géopolitique »*[1251]. Autrement dit, ce n'est plus seulement l'État qui dicte les règles techniques car dorénavant des coalitions privées multinationales élaborent de facto des standards qui deviennent la base même des infrastructures numériques. Les consortiums industriels se distinguent notamment par leur réactivité et leur orientation vers le marché, ils sont formés par des entreprises aux intérêts communs, et peuvent développer des normes très spécialisées plus rapidement que les organismes de normalisation traditionnels. Comme le note le rapport de Sorina Teleanu, ces arènes privées sont « *souvent vus comme moins bureaucratiques et plus efficaces pour réagir aux besoins du marché »*[1252]. Ainsi, des groupes tels que le W3C, l'OGC, Hyperledger (pour la blockchain), ou encore l'Industry IoT Consortium ont pour objectif de poser des règles d'interopérabilité et de sécurité spécifiques à leurs domaines, souvent sous forme de spécifications ouvertes ou open source. Par exemple, l'OGC se présente explicitement comme un moteur de l'innovation géospatiale mondiale, publiant des normes permettant des échanges d'informations transparentes entre systèmes. Dans le cloud, les fondations comme OpenStack ou CNCF (Kubernetes) fonctionnent sur ce modèle, elles rassemblent les fournisseurs et utilisateurs pour établir des plateformes de référence qui finissent par servir de standards de fait, même sans mandat étatique explicite.

Les stratégies diffèrent cependant selon les régions. En Europe, la volonté politique de souveraineté numérique oriente les consortiums vers des objectifs collectifs. L'axe franco-allemand porte le concept de « cloud souverain », traduisant une forte méfiance à l'égard des géants américains

[1251] Timmers Paul, « Géopolitique de la normalisation », EU cyber Direct, 9 avril 2020. https://eucyberdirect.eu/blog/geopolitic-de-la-normalisation. Consulté le 14 décembre 2022.

[1252] Teleanu Sorina, « The geopolitics of digital standards: China's role in standard-setting organisations », DiploFoundation/Geneva Internet Platform and Multilateral Dialogue Konrad Adenauer Foundation Geneva, 2021, p.5. https://www.diplomacy.edu/wp-content/uploads/2021/12/Geopolitics-of-digital-standards-Dec-2021.pdf.

du cloud. Alors qu'au même moment, le Royaume-Uni adopte une posture plus conciliante envers les fournisseurs US. La France et l'Allemagne soutiennent ainsi des projets comme GAIA-X ou la création de « data spaces » sectoriels, complétés par des réglementations (par exemple le label SecNumCloud de l'ANSSI) pour encadrer l'usage des technologies selon les valeurs européennes. En outre, les consortiums européens ont souvent un ancrage multipartite mêlant secteur public et privé, ce qui les distingue des modèles purement corporatifs.

Aux États-Unis, l'approche est plus libérale et dominée par les acteurs du marché. De nombreux standards émergent à travers des associations professionnelles ou fondations indépendantes, reflétant l'hégémonie technologique américaine. Par exemple, la Cloud Native Computing Foundation (CNCF), qui développe des normes pour les technologies Cloud a fait de Kubernetes le pilier de l'informatique en nuage, en rassemblant Google, AWS (Amazon) et Microsoft entre autres. Ces entités ont une portée mondiale, mais incarnent les visions de leurs fondateurs privés avant tout. La Chine, pour sa part, privilégie un modèle étatique, même au sein des consortiums et comités nationaux « privés ». Ces derniers sont systématiquement alignés sur les priorités du gouvernement. Beijing encourage la formation d'alliances domestiques, notamment pour pallier les ruptures technologiques imposées par les sanctions occidentales. L'OpenAtom Foundation, lancée en 2020 avec le soutien du ministère chinois, en est un exemple typique[1253]. Cette fondation regroupe Alibaba, Baidu, Huawei, Tencent et d'autres grands groupes pour développer des logiciels open source stratégiques [1254].

Cependant, si les consortiums privés créent de facto des standards parfois hégémoniques dans leurs domaines, et facilitent par là même l'interopérabilité à l'échelle mondiale, ils réduisent en parallèle l'espace d'intervention des politiques publiques. De plus, le fonctionnement parfois complexe des organes de normalisation et la prolifération des consortiums privés font qu'il est désormais difficile pour un pays seul de surveiller le développement de toutes les nouvelles normes. Cette émancipation du privé suscite également des interrogations sur l'accaparement de la normalisation par des intérêts marchands ou étatiques étrangers. Ainsi, si d'une part, les consortiums peuvent être perçus comme des leviers d'innovation agile et d'ouverture internationale, ils représentent également pour les États un défi à la souveraineté numérique. C'est une des raisons principales pour laquelle la diplomatie normative se retrouve aujourd'hui au cœur des stratégies étatiques. Il s'agit avant tout de réconcilier innovation et contrôle par la puissance publique. L'Union européenne, par exemple, cherche à exploiter ces consortiums pour projeter ses modèles à l'international, en s'appuyant sur le développement de normes

[1253] OpenAtom Foundation, Presentation and Governance Structure, Beijing, 2020, https://openatom.org. Consulté le 6 avril 2025.

[1254] OSCHINA, « Lancement de la première fondation open source chinois, « Open Atom Open Source Foundation (中国首个开源基金会 “开放原子开源基金会” 亮相) », 10 septembre 2020. https://www.oschina.net/news/118490/openatom-foundation-appeared. Consulté le 6 avril 2025.

ouvertes compatibles avec le RGPD ou les exigences de cybersécurité européennes. À l'inverse, la multiplication des consortiums privés multiple les « points de contact » multilatéraux, obligeant aussi les gouvernements à coopérer avec le privé sur la scène internationale. Dans les faits, les États n'ont plus le choix de s'intéresser au développement de normes par le secteur privé, qui reste aujourd'hui de loin le plus dynamique en matière de production normative. La prépondérance de l'OGC dans le développement de normes dans le domaine des données géographiques tend à démontrer qu'il n'échappe pas à ces logiques de compétitivité normative menée par le privé.

En définitive, les consortiums industriels jouent un rôle ambivalent. Ils structurent le cyberespace en normes concrètes, souvent bénéfiques pour l'interopérabilité et l'innovation, tout en faisant peser des enjeux de pouvoir sur l'échiquier global. Leur influence grandissante suggère que la souveraineté numérique ne peut plus être seulement une question de contrôle étatique traditionnel, mais doit intégrer la capacité des États à peser et à coopérer dans ces arènes privées transnationales. En plus des acteurs étatiques et des sociétés privées, un troisième groupe d'acteurs prend souvent part à des travaux entourant le développement de normes, notamment dans le domaine des données géographiques, il s'agit es chercheurs et universitaires. Souvent moins médiatisés que les autres acteurs, les alliances entre universités et acteurs privés ou étatiques jouent pourtant un rôle important dans le développement de normes novatrices.

2.3. Rôle des alliances universités-industries dans l'élaboration des normes

La normalisation technique joue un rôle central dans l'intégration des innovations numériques et géospatiales. Comme le soulignait déjà l'ingénieur américain pionnier dans le développement des micro-ordinateurs, Gordon Bell, en 1984, *« la normalisation est devenue aujourd'hui le problème le plus important dans la poursuite des progrès techniques »*[1255]. Les partenariats public-privé académiques ont toujours accompagné cette dynamique. Au-delà de la recherche pure, de nombreux organismes internationaux structurent la coproduction de standards. Par exemple, l'OGC se présente comme un « centre de confiance pour la collaboration » réunissant gouvernements, entreprises, universités et startups autour de défis mondiaux (changement climatique, urbanisme, sécurité alimentaire…). De même, l'ISO/TC 211 collabore étroitement avec l'OGC, des agences de l'ONU (FAO, Union postale universelle) et des associations scientifiques (Association internationale de géodésie, CEOS, GÉO…) pour développer des normes interopérables de données géospatiales. Ces alliances concrètes montrent que la recherche universitaire et l'industrie se mobilisent conjointement pour bâtir les standards techniques et permettre l'échange fluide de données.

Dans la pratique, de nombreux domaines illustrent ces alliances. En géomatique, aux consortiums mondiaux s'ajoutent des initiatives régionales, comme la directive INSPIRE européenne et les travaux de l'ONU sur les métadonnées spatiales, où universités et entreprises participent à la normalisation des formats de données. En intelligence artificielle, des alliances académiques-industrielles se structurent pour élaborer des standards et bonnes pratiques. Par exemple, à Paris-Saclay, le DataIA-Cluster regroupe 14 établissements d'enseignement et de recherche avec des industriels, dans le cadre du programme « France 2030 », avec pour objectif de faire de la France un « leader mondial en IA » tout en prenant en compte l'éthique et la souveraineté numérique[1256]. Ce type de pôle illustre comment des instituts de recherche coopèrent avec l'industrie pour cocréer des normes émergentes. En cybersécurité, les organismes de standardisation et les agences de normalisation associent universités et entreprises dans l'élaboration de référentiels de certifications cyber. De tels consortiums publics-privés visent à aligner exigences gouvernementales et contributions de la

[1255] Bell Gordon, cité dans : Rauf Gönenç, « Enjeux industriels des normes dans les technologies de l'information », in *Revue d'économie industrielle*, n° 39, 1987, pp. 208 – 2019, p. 208. https://www.persee.fr/doc/rei_0154-3229_1987_num_39_1_1251. Consulté le 21 mai 2023.

[1256] Ministère de l'Économie, « Mise en place du dispositif IA-Cluster pour soutenir l'intelligence artificielle », Direction Générale des Entreprises, 16 juin 2023. https://www.entreprises.gouv.fr/la-dge/actualites/mise-en-place-du-dispositif-ia-cluster-pour-soutenir-lintelligence-artificielle. Consulté le 10 décembre 2024.

recherche. Dans d'autres secteurs, blockchain, cloud, open data, les partenariats se développent également. À titre d'exemple, l'initiative européenne GAIA-X fédère un grand nombre d'industriels, d'institutions et d'universités autour de normes de cloud décentralisé, tandis que les universités contribuent à des projets open data définissant leurs propres guides ou adhérant aux Open Data Charter.

Sur le plan géographique, les dynamiques varient selon les régions. Aux États-Unis, la standardisation numérique reste largement pilotée par le privé (industries de la tech, consortiums comme l'IEEE, W3C, IETF…), soutenu par des instances fédérales (NIST, DARPA) qui stimulent la recherche académique via financements et appels à commentaires. En Europe, l'approche est plus multilatérale. Des comités techniques associent États membres, industriels et laboratoires publics. La France, historiquement très active, occupe ainsi le 2e rang au niveau européen en termes d'influence normative[1257]. En Chine, l'État encadre fermement la normalisation, comme démontré précédemment l'approche chinoise de la normalisation de l'IA est *« pilotée par l'État et menée par les entreprises »*[1258]. Beijing coopère étroitement avec ses géants technologiques dans une « communauté de pratique » où l'État joue tour à tour catalyseur, soutien et superviseur des normes naissantes. L'Inde et d'autres pays d'Asie du Sud mettent en place des comités nationaux et des incubateurs universitaires pour définir des standards locaux en 5G, IA et cybersécurité, souvent en partenariat avec l'industrie locale ou étrangère. En Afrique subsaharienne, les efforts normatifs passent surtout par des projets de formation et d'infrastructures géospatiales via des centres régionaux de recherche, et la participation aux travaux de l'UN-GGIM Afrique, plutôt que par des consortiums formalisés.

Plusieurs pôles géographiques et lieux de coconstruction des normes se distinguent. Aux États-Unis, les écosystèmes de la Silicon Valley, de Seattle ou de la région Boston-Cambridge forment des hubs technologiques où convergent universités de pointe et entreprises majeures comme Apple, Google, IBM, ou encore Microsoft. Ces territoires sont aussi le siège d'instituts de normalisation privés comme l'IEEE, le W3C, et des consortiums industriels. En Europe, outre Bruxelles, des clusters régionaux émergent comme à Paris-Saclay (data science et IA) ou Sophia Antipolis en cybersécurité, où les laboratoires universitaires sont mis en réseau avec des startups et des centres de recherche publics. En Asie, la Tech Valley de Shenzhen et le corridor Tokyo-Yokohama (Japon), de même que Bangalore à Hyderabad (Inde) et Singapour, combinent universités techniques et clusters industriels pour travailler sur des normes émergentes. Ces hubs concentrent ressources et expertise, les universités y fournissent la recherche fondamentale et la formation de chercheurs, tandis que les entreprises

[1257] Booz Allen Hamilton / NASA, *Geospatial Interoperability Return on Investment Study*, NASA Geospatial Interoperability Office, avril 2005 ; voir également : NATO ACT, *Allied Command Operation Geospatial Handbook*, Naples, 2009, p. 12.

[1258] Finnish Institute of International Affairs, « China's approach to AI standardisation: State-guided but enterprise-led », FIIA Briefing Paper, n° 391, août 2024. https://fiia.fi/en/publication/chinas-approach-to-ai-standardisation.

apportent leurs cas d'usage et leur capacité de mise en œuvre, facilitant ainsi la co-élaboration des standards.

La gouvernance mondiale des normes technologiques liées aux données géographiques numériques résulte donc d'un jeu complexe impliquant les États, les consortiums privés et les alliances académiques. D'un côté, la diplomatie normative des gouvernements agit dans les enceintes internationales pour imposer des standards conformes à leurs intérêts. L'Union européenne, par exemple, est présentée comme *« puissance normative qui exporte ses standards et ses normes »* via son vaste marché stable et ses accords commerciaux [1259]. Les États-Unis misent en revanche sur leurs entreprises globales. Ainsi, des plateformes comme Google ou Microsoft, tout en étant privées, opèrent mondialement, collectent d'immenses volumes de géodonnées et imposent de facto leurs propres formats et protocoles [1260]. Les pays occidentaux cherchent aujourd'hui à créer ou exporter leurs normes techniques et juridiques (directives européennes INSPIRE pour les géodonnées, RGPD pour la vie privée, architectures de cloud souverain). Toutefois, comme le souligne Douzet, la dépendance européenne aux acteurs américains reste très forte, et les États européens restent fortement dépendants des plateformes américaines, sur lesquelles ils n'ont aucun contrôle direct [1261]. Au contraire, la Chine a favorisé le développement de ses propres plateformes nationales avec le soutien de l'État, captant l'essentiel du trafic intérieur. De ce fait, les normes géospatiales en Chine sont souvent endogènes et promues via des réseaux d'influence, comme la NRS, alors qu'en Europe et en Amérique du Nord les standards tendent à être négociés dans des forums multilatéraux ou issus du marché global. Les pays émergents, eux, sont généralement moins actifs dans l'élaboration des normes et doivent s'appuyer sur des cadres internationaux existants. Sous l'égide de l'ONU et d'organismes comme UN-GGIM, ces derniers sont encouragés à adopter des normes ouvertes afin que ces pays ne soient pas oubliés dans la gestion de l'information géospatiale [1262]. De fait, la réduction de la fracture numérique passe par l'adhésion à des standards communs qui facilitent le partage et l'intégration des données à tous les niveaux géographiques.

Cette situation multiscalaire entraîne des tensions, mais aussi des complémentarités entre acteurs publics, privés et académiques. Les États veulent préserver leur souveraineté et, pour ce faire, ils encadrent la localisation des infrastructures, la protection des géodonnées sensibles ou l'accès à

[1259] Bermann Sylvie, et Fabry Elvire, « Construire l'autonomie stratégique de l'Europe face à la Chine », Institut Jacques Delors, rapport n° 124, décembre 2021, p. 12. https://institutdelors.eu/wp-content/uploads/2021/12/R124_Construire_autonomie_Europe_face_Chine_Interactif.pdf.

[1260] Douzet Frédéric et Desforges Alix, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », Expéditions géographiques en Terres numériques, fronts pionniers et nouvelles limites - Hommage à Henry Bakis, NETCOM, n° 32, 2018, pp. 87 – 108. https://journals.openedition.org/netcom/3419?lang=fr. Consulté le 21 mars 2023.

[1261] *Ibid*

[1262] UN GGIM, « A Guide to the Role of Standards in Geospatial Information Management », février 2022. https://ggim.un.org/Revised-Standards-Guide/.

certaines fréquences, alors que les entreprises plaident pour la fluidité des marchés et défendent souvent des formats propriétaires ou des brevets technologiques. Dans ce conflit potentiel, les universités jouent un rôle de stabilisation. Elles poussent pour le développement de normes interopérables et la neutralité technique, et elles forment les futurs experts en normalisation. De plus, la mise en œuvre concrète des standards se fait souvent par coopération. Ainsi, l'OGC regroupe agences publiques, entreprises et laboratoires pour élaborer ensemble des spécifications communes. Des projets européens de recherche financent des partenariats R&D entre universités et industrie et des commissions mixtes internationales, comme la Global Commission on the Stability of Cyberspace, qui réunissent des experts issus des milieux industriel, académique et gouvernementaux pour dégager des principes normatifs dans le cyberespace. Ces alliances révèlent que, malgré la concurrence, les intérêts stratégiques convergent vers un besoin partagé de normes robustes. Ainsi, comme le rappellent Douzet et Desforges, *« les chercheurs possèdent… des compétences »* [1263]et la *« légitimité historique »* [1264]sur les réseaux numériques, tandis que les grandes entreprises, grâce à leur visibilité sur les flux de données, sont « *des partenaires essentiels dans la mise en œuvre des normes »* [1265].

Ces observations ont des implications directes pour la souveraineté numérique française et européenne. L'UE dispose d'un fort levier normatif, mais elle doit l'exercer davantage pour préserver son autonomie stratégique. Un rapport de l'Institut Montaigne note que le principal atout de l'UE est d'être le plus grand marché mondial stable, d'où sa capacité à imposer des standards par son droit interne et ses accords commerciaux [1266]. En pratique, cela implique de soutenir activement les processus normatifs internationaux et d'investir dans les acteurs domestiques pour qu'ils puissent représenter les intérêts français et européens. L'expérience récente montre en effet la fragilité d'une souveraineté numérique fondée sur des technologies externes. En France, par exemple, *« les plateformes américaines captent 78 % de toutes les visites »*[1267] Internet, illustrant une dépendance techno-économique. Pour y remédier, la France et l'Europe doivent renforcer leur écosystème technologique tout en continuant de prôner des normes ouvertes et éthiques. Plus largement, l'évolution de la normalisation numérique soulève des enjeux géopolitiques, économiques et scientifiques majeurs. Cette dynamique nourrit les rivalités entre grandes puissances, chacune cherchant à imposer ses propres standards technologiques ou éthiques, mais aussi crée des opportunités de coopération scientifique. Des standards ouverts et harmonisés facilitent, par exemple, la recherche internationale et soutiennent le

[1263] Douzet Frédéric et Desforges Alix, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », Expéditions géographiques en Terres numériques, fronts pionniers et nouvelles limites - Hommage à Henry Bakis, NETCOM, n° 32, 2018, pp. 87 – 108. https://journals.openedition.org/netcom/3419?lang=fr. Consulté le 21 mars 2023.

[1264] Ibid

[1265] Ibid

[1266] Institut Montaigne, *Souveraineté numérique : reprendre le contrôle ?*, Paris, octobre 2020, pp. 34–38.

[1267] ARCEP / CREDOC, *Baromètre du numérique — Édition 2022*, Paris, 2023, p. 47 ; Voir aussi StatCounter Global Stats, Search Engine Market Share France, janvier 2022

développement technologique. À l'inverse, des normes fragmentées ou dominées par quelques acteurs peuvent limiter l'innovation et accroître les dépendances stratégiques. La gouvernance des normes numériques apparaît donc comme un enjeu central pour la souveraineté, et la France et l'Union européenne ont tout intérêt à mobiliser l'ensemble des leviers, diplomatique, industriel et académique, afin de peser sur l'architecture normative globale.

En conclusion, il apparaît évident que l'Europe se doit de consolider sa puissance normative en faisant valoir des standards qui reflètent ses valeurs et en formant des coalitions avec des partenaires partageant ces principes. D'autre part, le renforcement des alliances université-industrie est crucial. Les programmes conjoints doivent être stimulés pour innover dans la normalisation elle-même. Enfin, la France doit utiliser sa position dans des organisations comme l'AFNOR ou l'ETSI pour influencer les normes en gestation et encourager l'interopérabilité des systèmes. En somme, la souveraineté numérique passe par une stratégie combinant action publique, initiative privée et coopération académique. Une telle approche intégrée permettra de renforcer l'influence normative de la France et de l'Europe dans le cyberespace, face à la montée en puissance des normes non européennes et aux défis géopolitiques émergents.

3. Quel futur pour la normalisation de défense ?

Les besoins de la défense en matière de normalisation des données appliquées aux données géographiques continuent à être une priorité pour le ministère des armées. Les travaux dans ce domaine aident le Ministère à analyser les spécifications ou projets de spécifications qui concernent ses besoins au regard des évolutions actuelles dans ce domaine. Au vu de l'aggravation des tensions internationales et l'accélération des projets de modernisation technologique entrepris par les armées, la normalisation des données géographiques est une étape capitale pour le déploiement de ces technologies. La normalisation de ces données doit également permettre le développement de profils de défense de ces normes de nouvelle génération, en renforçant l'interopérabilité, non seulement au sein des armées, mais également entre tous les partenaires de la France, en particulier au sein de l'OTAN. La veille technologique en matière de normalisation constitue également un autre aspect important dans ce domaine pour que les armées françaises puissent bénéficier des normes les plus appropriées et performantes au vu des enjeux de demain.

De plus, avec le développement du concept de Numérisation de l'Espace de Bataille, les besoins en matière de disponibilité d'un grand nombre d'informations provenant de différentes sources se sont singulièrement accrus ces dernières années. La normalisation des données doit donc permettre de faciliter l'accès et la diffusion de ces données entre toutes les armes. Le ministère des Armées a donc besoin de suivre les travaux en cours en matière de normalisation, afin de s'assurer de leur compatibilité avec les orientations nationales. Par ailleurs, l'interopérabilité entre les différentes communautés marine et aéroterrestre doit être favorisée, ce qui implique entre autres une collaboration entre le DGIWG, et l'OGC ou encore l'IHO. L'objectif est d'assurer l'interopérabilité entre les systèmes d'information du ministère des Armées relativement aux données GHOM (Géographique, Hydrographique, Océanographique et Météorologique), et ainsi maîtriser l'environnement géophysique dans le contexte d'intervention. Ainsi, toutes les armées sont concernées par les enjeux de la normalisation des données géographiques, et chaque aspect de cette normalisation est mobilisé.

3.1. Des défis en matière de normalisation pour l'ensemble des armées

Certains travaux de normalisation touchent à des dimensions universelles pour les données manipulées, quelles que soient les armes qui les emploient en priorité. Ceux entourant la qualité des données, les métadonnées ou encore les représentations cartographiques (portrayal) rentrent dans cette catégorie.

Dans les systèmes de données géospatiales contemporains, la notion de qualité ne peut pas être abordée comme un simple critère annexe ou secondaire. Elle s'impose au contraire comme un pilier fondamental de l'interopérabilité, de la confiance informationnelle et de l'optimisation décisionnelle, en particulier dans les environnements de Défense, où la précision, la fiabilité et la traçabilité des informations conditionnent directement l'efficacité des actions menées. Les normes internationales, en particulier celles issues de l'ISO TC 211 (notamment la série ISO 19157)[1268], de l'OGC, de l'OTAN (STANAG 2215)[1269], ou du DGIWG, proposent un cadre conceptuel unifié pour structurer la qualité des données selon des dimensions multiples : exactitude, cohérence logique, exhaustivité, pertinence temporelle, et utilisabilité. Ces paramètres permettent d'élaborer des métadonnées qualité, des rapports d'évaluation, ou des couches de qualification exploitables par des systèmes d'analyse ou de visualisation.

Cependant, la simple existence de ces standards ne suffit pas à garantir leur application homogène ni leur pertinence contextuelle. Les enjeux majeurs résident dans leur mise en œuvre opérationnelle, leur interprétation nationale et leur adaptation aux processus de production, de transformation ou d'exploitation des données. La diversité des formats, la multiplication des sources, et l'accroissement des volumes imposent de repenser l'approche classique fondée uniquement sur les métadonnées statiques. Deux tensions fondamentales structurent aujourd'hui les débats : d'un côté, le besoin d'une standardisation rigoureuse, pour permettre la comparaison entre jeux de données produits dans différents contextes ou par différentes nations, et de l'autre, la nécessité d'une souplesse d'adaptation, notamment à travers le développement de guides d'implémentation. Ce dernier point est crucial pour les programmes de géographie militaire, où la qualité doit être compréhensible et exploitable à la fois par les producteurs et les utilisateurs, dans un langage partagé, mais adaptable. Dans ce cadre, les normes comme ISO 19157-1 : 2023[1270] apportent des avancées notables pour

[1268] ISO 19157-1 : 2023 Informations géographiques — Qualité des données. Partie 1: Exigences générales, 2023. https://www.iso.org/fr/standard/78900.html.

[1269] STANAG 2215 Évaluations des Cartes terrestres, des Cartes aéronautiques et des Données topographiques numérisées, Ed. 7, 13 juin 2020. https://standards.globalspec.com/std/1296998/stanag-2215.

[1270] ISO 19157-1 : 2023 Informations géographiques — Qualité des données. Partie 1: Exigences générales, 2023. https://www.iso.org/fr/standard/78900.html.

l'évaluation de la qualité des données : simplification du modèle, prise en compte des retours utilisateurs, intégration de résultats de qualité sous forme de couches. Toutefois, leur mise en œuvre reste techniquement complexe et nécessite des outils adaptés ainsi que des accompagnements documentaires (guides, profils nationaux, retours d'expérience). À ce titre, la norme ISO/TS 19158[1271] comble un vide en définissant des protocoles d'assurance qualité dans la relation fournisseur-utilisateur, incluant des niveaux d'accréditation et des mécanismes de confiance.

En parallèle, les réflexions actuelles au sein de l'OGC introduisent des notions émergentes, comme l'IPT (Integrity, Provenance, Trust), qui visent à étendre le champ de la qualité à des dimensions jusqu'ici peu modélisées. L'intégrité fait référence à l'absence d'anomalie, la provenance, à la traçabilité des données, la confiance, et à la capacité d'utiliser l'information comme aide à la décision. Ces axes illustrent une évolution vers une conception plus relationnelle et situationnelle de la qualité, intégrée dans les chaînes de traitement en temps réel, et non uniquement dans des audits a posteriori.

Malgré ces dynamiques, plusieurs freins subsistent. Tout d'abord, la faible lisibilité des normes ISO pour les acteurs de terrain, le manque de convergence entre l'ISO et l'OGC, la rareté des outils de validation interopérables, ou encore la réticence des États à investir dans l'adaptation nationale des profils qualité. À cela s'ajoute l'absence d'un registre mondial consolidé de mesures de qualité (en cours de développement via ISO 19157-3[1272]), capable de garantir la stabilité sémantique et la durabilité des indicateurs utilisés. La situation actuelle révèle donc un écart préoccupant entre les standards disponibles et leur exploitation effective, notamment dans les forces armées. À cet égard, la position française se caractérise par une volonté de structurer une gouvernance qualité adaptée à ses spécificités stratégiques : développement de guides, contributions aux normes internationales, participation aux groupes de travail sur les métadonnées, notamment via le groupe de travail du CNIG QuaDoGéo[1273], et intégration des exigences qualité dans les processus de production de données. Cette stratégie cherche à éviter l'écueil d'une standardisation abstraite ou théorique, en lui donnant une portée pratique et souveraine.

Les métadonnées jouent plusieurs rôles stratégiques afin d'assurer l'interopérabilité des données géographiques. D'une part, elles assurent la traçabilité des processus de production, depuis l'acquisition jusqu'à la diffusion. D'autre part, elles sont indispensables pour garantir que les utilisateurs disposent d'une information contextualisée, fiable et conforme aux exigences spécifiques

[1271] ISO/TS 19158:2012 Information géographique — Assurance qualité relative à l'approvisionnement de données, Ed. 1, 2012. https://www.iso.org/fr/standard/32576.html.

[1272] ISO/DIS 19157-3 Information géographique — Qualité des données. Partie 3: Registre des mesures de la qualité des données, en cours de développement.

[1273] Conseil National de l'Information géoréférencée (CNIG), « Quadogéo », 28 mai 2025. https://cnig.gouv.fr/gt-quadogeo-a18183.html

des opérations militaires. Elles contribuent également à organiser l'accès aux données via des services de catalogage, désormais au cœur des infrastructures géospatiales modernes. Aujourd'hui, le socle normatif international repose essentiellement sur la série de normes ISO 19115[1274], qui définit le modèle conceptuel des métadonnées pour les ressources géographiques. La version actuelle, ISO 19115-1 : 2014[1275], constitue une refonte majeure de la norme initiale (ISO 19115:2003) et introduit des améliorations notables dans la structuration de l'information descriptive. Cette norme est complétée par ISO 19115-2[1276] pour les données d'acquisition et d'imagerie, ainsi que par ISO 19157[1277] pour la description de la qualité des données. Les implémentations XML sont précisées par ISO 19115-3[1278], garantissant une correspondance stricte entre le modèle UML et les schémas XML utilisés dans les échanges numériques. Cette cohérence technique est indispensable pour assurer l'interopérabilité entre producteurs, systèmes et utilisateurs.

Au-delà de ces normes génériques, les besoins spécifiques des forces armées sont couverts par des profils spécialisés, adaptés au contexte opérationnel. Le DGIWG Metadata Foundation (DMF)[1279] constitue le profil de référence pour la Défense. Construit à partir des normes ISO précitées, DMF organise l'ensemble des éléments descriptifs nécessaires aux données géographiques militaires. Il intègre des métadonnées sur la provenance, les conditions d'utilisation, les niveaux de qualité, ainsi que des informations de sécurité adaptées aux contraintes des opérations interarmées. Le NATO Geospatial Metadata Profile (NGMP)[1280], encadré par le STANAG 2586, décline ces exigences au sein de l'OTAN. Ces profils sont essentiels pour garantir que les métadonnées produites par les forces françaises s'intègrent pleinement dans les chaînes OTAN, tout en conservant la spécificité des besoins nationaux.

Cependant, les métadonnées n'ont de valeur que si elles sont exploitables par des services permettant leur découverte et leur accès. C'est le rôle des services de catalogage, historiquement fondés sur le protocole CSW (Catalogue Service for the Web)[1281], normalisé par l'OGC. Des déclinaisons spécifiques, telles que le profil d'application ISO de CSW, permettent d'assurer la compatibilité avec les normes ISO 19115. Cependant, ces solutions traditionnelles évoluent aujourd'hui vers des API

1274 ISO 19115-1 : 2014 Informations géographiques — Métadonnées, Ed. 1, 2014. https://www.iso.org/fr/standard/53798.html

1275 ISO 19115-1 : 2014 Informations géographiques — Métadonnées. Partie 1: Principes de base, Ed. 1, 2014. https://www.iso.org/fr/standard/53798.html

1276 ISO 19115-2 : 2019 Informations géographiques — Métadonnées. Partie 2: Extensions pour l'acquisition et le traitement. https://www.iso.org/fr/standard/67039.html

1277 ISO 19115-3 : 2023 Informations géographiques — Métadonnées. Partie 3: Mise en œuvre par des schémas XML. https://www.iso.org/fr/standard/80874.html

1278 DGIWG 114 : DGIWG Metadata Foundation, Ed. 2, 12 juillet 2017.

1279 https://dgiwg.org/documents/dgiwg-standards

1280 NATO STANDARD AgeoP-08 NATO Geospatial Metadata Profile, Ed B, Version 1, février 2019. https://nso.nato.int/nso/nsdd/main/standards/ap-details/2769/EN

1281 OGC Catalogue Services 3.0 - General Model, 12-168r6, 10 juin 2016.http://docs.opengeospatial.org/is/12-168r6/12-168r6.html.

modernes, en particulier OGC API Records[1282], qui vise à remplacer CSW en s'appuyant sur des technologies Web contemporaines. Cette évolution est cruciale pour permettre l'intégration des services de catalogage dans les architectures de données actuelles. Parallèlement, les travaux autour de GeoDCAT[1283], extension géospatiale du vocabulaire DCAT[1284] du W3C, ouvrent la voie à une convergence entre le monde des infrastructures de données spatiales et celui des données ouvertes (Open Data) ou du Linked data (données liées), anticipant des usages futurs dans les échanges entre les sphères civiles et militaires.

Les enjeux de normalisation des métadonnées pour la Défense vont bien au-delà des aspects techniques. Ils touchent directement à la souveraineté numérique, à l'interopérabilité interalliée, et à la capacité d'action autonome des forces françaises sur les théâtres d'opérations. La convergence progressive vers des modèles communs (ISO 19115-1, DMF, NGMP), associée au développement de services modernes (OGC API Records, GeoDCAT), constitue une opportunité majeure pour la Défense de moderniser ses chaînes de gestion de l'information géospatiale. Toutefois, cette transition implique un investissement continu dans les instances de normalisation, un pilotage rigoureux des profils d'application, et une stratégie affirmée de coordination nationale. Dans ce contexte, le succès repose sur trois leviers fondamentaux : l'anticipation des évolutions technologiques, la cohérence entre normes civiles et profils militaires, et la défense active des besoins nationaux dans les enceintes internationales. La coexistence de multiples standards de représentation graphique de l'information géospatiale illustre un paysage normatif fragmenté, au sein duquel se croisent des héritages techniques anciens, des dynamiques institutionnelles complexes et des intérêts industriels souvent divergents. Ce morcellement structurel constitue un frein majeur à l'interopérabilité des systèmes, en particulier dans les contextes à forte contrainte opérationnelle, tels que les environnements de défense. Les standards historiques, tels que GEOSYM, le Vector Product Format (VPF), ou les spécifications des MIL STD américaines, ont été conçus dans un paradigme essentiellement statique, où la priorité était donnée à la standardisation de produits cartographiques finis, destinés à un usage fermé, souvent papier ou limité à des infrastructures propriétaires. Si ces référentiels ont joué un rôle structurant dans la mise en place d'un

[1282] OGC API - Records - Part 1: Core, 5 février 2025. https://docs.ogc.org/is/20-004r1/20-004r1.html

[1283] Le 18 mai 2023, l'OGC a annoncé la création d'un groupe de travail centré sur le développement d'un profil géographique pour DCAT, un vocabulaire permettant de décrire les ensembles de données et les services, et le principal moyen de cataloguer les ensembles de données sur le Web. Source : https://www.ogc.org/fr/announcement/ogc-forms-new-geodcat-standards-working-group/

[1284] Data Catalog Vocabulary (DCAT) est un vocabulaire RDF conçue pour faciliter l'interopérabilité entre les catalogues de données publiées sur le Web. DCAT permet à un éditeur de décrire des ensembles de données et des services de données dans un catalogue à l'aide d'un modèle et d'un vocabulaire standard qui facilite la consommation et l'agrégation de métadonnées provenant de plusieurs catalogues. Cela peut améliorer la découverte des ensembles et des services de données. Il permet également une approche décentralisée de la publication des catalogues de données et rend possible la recherche fédérée d'ensembles de données dans les catalogues de plusieurs sites en utilisant le même mécanisme et la même structure d'interrogation. Les métadonnées DCAT agrégées peuvent servir de fichier manifeste dans le cadre du processus de conservation numérique. Source : https://www.w3.org/TR/vocab-dcat-3/

langage cartographique commun au sein des forces armées occidentales, ils souffrent aujourd'hui d'un décalage croissant vis-à-vis des exigences contemporaines en matière de souplesse d'affichage, d'accessibilité Web, de représentations dynamiques et de visualisation à la demande.

En réponse à cette obsolescence, de nouvelles initiatives cherchent à redéfinir le cadre normatif autour de concepts plus modulaires et adaptatifs. L'émergence de modèles comme SymCore (Symbology Conceptual Model ou Modèle conceptuel de Symbologie)[1285] et le développement d'interfaces normalisées via les OGC API (styles, Maps, Features) témoignent de cette tentative de refondation. Ces standards, conçus autour de classes abstraites et d'encodages flexibles (CSS, JSON, XML), visent à offrir des solutions capables de répondre aux besoins croissants de visualisation contextuelle, d'indépendance vis-à-vis des formats propriétaires et d'intégration dans des services interopérables. Toutefois, malgré leurs potentialités techniques, ces nouvelles normes peinent à se généraliser, en raison d'un déficit de maturité opérationnelle, d'un manque d'implémentations industrielles robustes, mais aussi en raison des logiques de verrouillage institutionnel entretenues par les standards dominants existants. C'est dans ce contexte que certaines nations, dont la France, se positionnent comme des forces motrices de modernisation normative. Forte de son expérience dans des programmes tels que GEODE 4D ou GeoMaps, la France développe des approches méthodiques de représentation cartographique répondant simultanément aux besoins d'efficacité militaire et aux exigences d'interopérabilité multinationale. En anticipant les lacunes des normes en vigueur, elle contribue activement à l'élaboration de recommandations techniques, à la révision de spécifications anciennes et à l'expérimentation de démonstrateurs intégrant des capacités avancées de symbologie.

Cependant, cette impulsion réformatrice se heurte à plusieurs résistances. Sur le plan institutionnel, les forums internationaux de normalisation restent marqués par des inerties procédurales et des rapports de force historiques. Les positions dominantes acquises par certains acteurs industriels, notamment des éditeurs de logiciels propriétaires comme ESRI, peuvent également freiner l'adoption de normes ouvertes qui remettraient en cause leur modèle économique. D'un point de vue stratégique, les pays qui ont investi massivement dans des infrastructures de données alignées sur des standards anciens peuvent être réticents à réorienter leur trajectoire technique vers des modèles encore en cours de stabilisation.

[1285] OGC Symbology Conceptual Model: Core Part, 18-067r3, 15 octobre 2020. http://www.opengis.net/doc/IS/SymCore/1.0

3.2 La normalisation militaire au défi de la mise en réseau des armes dans tous les domaines

Dans le domaine hydrographique, la spécification S-100 constitue le cadre de référence pour les données géospatiales appliquées à l'hydrographie numérique. Elle a été choisie pour structurer une large variété de sources de données numériques dans ce domaine. Conçue en conformité totale avec les standards géospatiaux mondiaux, notamment ceux de la série ISO 19100, elle facilite l'interopérabilité des systèmes et l'intégration des données hydrographiques dans les environnements géospatiaux existants. Cette norme englobe une famille de spécifications appelées S-1xx, chacune définissant un type de produit basé sur le socle S-100[1286]. Ces produits sont destinés à alimenter les prochaines générations de systèmes ECDIS (Electronic Chart Display and Information Systems), en appui à l'initiative globale de navigation électronique. Celle-ci vise à harmoniser la collecte, la gestion, la diffusion et l'affichage d'informations maritimes à bord et à terre, au moyen de technologies numériques, dans le but d'améliorer la sécurité, la sûreté maritime et la protection de l'environnement. La version 4.0.0 de la norme S-100 a été officialisée en décembre 2018, avec un texte disponible sur le nouveau portail de l'OHI. Une mise à jour numérotée 5.2.0 a été publiée en juin 2024. Enfin, à compter du 1er janvier 2029, les nouveaux systèmes devront impérativement respecter la nouvelle résolution de l'Organisation maritime internationale sur les critères de performance des ECDIS. À ces standards de l'IHO s'ajoutent les STANAGs développés au sein de l'OTAN concernant les données hydrographiques. Ainsi, l'OTAN a publié deux principaux standards dans le domaine de l'hydrographie basé sur les normes S-100 et S-57[1287] de l'OHI : le DMGEM (Defense Maritime Geospatial Exchange Model)[1288] et les AML (Additional Military Layer)[1289].

Le modèle d'échange des données géospatiales maritimes à finalité militaire, désigné sous l'acronyme DMGEM, a été élaboré afin de répondre aux impératifs d'interopérabilité spécifiques aux

---

[1286] International Hydrographic Organisation, Universal Hydrographic Data Model, Ed. 5.2.0, juin 2023. https://iho.int/fr/normes-et-specifications.

[1287] International Hydrographic Organisation, Normes de l'OHI pour le transfert de données hydrographique numérique, Ed. 3.1, novembre 2000. https://iho.int/fr/normes-et-specifications

[1288] L'objectif du DMGEM est de spécifier le contenu, la structure et la représentation des produits de données géospatiales destinés à être utilisés dans un large éventail de systèmes. Ces produits permettent à l'utilisateur maritime de la défense d'avoir une bonne connaissance de la situation dans toute la gamme des opérations maritimes (AJP-3.1), à tous les niveaux opérationnels, de la planification stratégique à l'opération tactique. Voir : NATO – AGEOP-14, Defence Maritime Geospatial Exchange Model, Embracing S-100 and NGIF Developments. https://standards.globalspec.com/std/10266602/ageop-14

[1289] Les AML sont une *« gamme cohérente de produits numériques géoréférencés conçus pour satisfaire l'ensemble des besoins maritimes de défense de l'OTAN autres que la navigation »*. Source: Vos Elen, « Additional Military Layer », IHO, 2013. https://legacy.iho.int/mtg_docs/com_wg/TSMAD/TSMAD26/presentations/GMWG_Brief_on_AML2TSMAD.pdf

environnements maritimes de défense. Il s'inscrit dans la continuité du cadre géospatial de l'OTAN et se conforme aux orientations définies par la directive géospatiale MC 0296, qui consacre le principe opérationnel fondamental de *« combattre sur une carte commune »*[1290]. Ce dispositif vise à pallier les insuffisances identifiées dans la NATO Geospatial Deficiencies Matrix (NGDM) en fournissant un cadre structurant pour la conception des spécifications de produits géospatiaux de type AML+ (Additional Military Layers Plus). Ces spécifications sont destinées à l'élaboration de jeux de données adaptés aux systèmes de commandement et de contrôle (C2), ainsi qu'aux WECDIS (Warship Electronic Chart Display and Information Systems)[1291], systèmes de visualisation électronique des cartes marines employées à bord des bâtiments de guerre. Le STANAG 7170[1292], placé sous la coordination du Royaume-Uni par l'intermédiaire de l'United Kingdom Hydrographic Office (UKHO), vise à l'élaboration d'un ensemble cohérent de produits numériques intégrés répondant à des besoins opérationnels étroitement liés à la navigation. Ce standard a pour objectif principal de fournir des outils numériques avancés facilitant la compréhension de l'environnement opérationnel (situational awareness) grâce à la représentation visuelle de données géospatiales, ainsi que de soutenir les processus de planification et de prise de décision dans le cadre des opérations militaires. En parallèle de ces développements, l'OGC travaille actuellement sur le standard CF-netCDF[1293] (Network Common Data Form)[1294]. Le standard CF-netCDF constitue un ensemble de spécifications destinées à l'encodage de données géospatiales numériques représentant des phénomènes évoluant dans l'espace et dans le temps. Initialement conçu pour répondre aux besoins de la communauté des sciences de la Terre, le format netCDF s'est progressivement imposé comme un outil polyvalent pour la représentation, le stockage et l'échange de données multidimensionnelles. Son modèle de données ainsi que ses mécanismes de codage sont particulièrement prisés dans les disciplines scientifiques liées à l'atmosphère et à l'océan, où ils facilitent la gestion et l'analyse de grands ensembles de tableaux de données corrélés.

[1290] Sprival Andris, « Geographic Support Requirements For Future NATO Joint Expeditionary Missions », Estonian Journal of Military Studies, Volume 1, 2016, pp. 11–40, p. 3. https://www.ksk.edu.ee/wp-content/uploads/2016/02/S%C3%B5jateadlane_1_02_Sprivul.pdf. Consulté le 12 mars 2025.

[1291] Northrop Grumman, « Warship Electronic Chart Display and Information System (WECDIS) », 2013, p.2. http://www.vscomm.co.th/storage/product/2025/01/9b17932db9116262b6ea836a063418fa.pdf

[1292] NATO - STANAG 7170, Additional Military Layers (AML) – Digital Geospatial Data Products, pp. 7, 22 février 2022. https://standards.globalspec.com/std/14501420/stanag-7170.

[1293] OGC, OGC Network Common data Form (NetCDF) Core Encoding Standard version 1.0., 4 mai 2011. https://www.ogc.org/standards/netcdf/

[1294] NetCDF (Network Common Data Form) est un ensemble de bibliothèques logicielles et de formats de données indépendantes de la machine qui permettent la création, l'accès et le partage de données scientifiques. Il s'agit également d'une norme communautaire pour le partage des données scientifiques. Le centre de programme Unidata supporte et maintient les interfaces de programmation netCDF pour C, C++, Java et Fortran. Des interfaces de programmation sont également disponibles pour Python, IDL, MATLAB, R, Ruby et Perl. Source : https://www.unidata.ucar.edu/software/netcdf/.

Dans le champ des systèmes d'information géographique appliqués aux besoins militaires, la normalisation des données géographiques vecteurs constitue également un enjeu stratégique décisif. Ces données, représentant sous forme d'objets géométriques les éléments physiques et fonctionnels du terrain, sont au cœur des systèmes d'aide à la décision, des dispositifs de commandement et des systèmes d'armes modernes. Leur structuration et leur échange dans des formats cohérents, interopérables et robustes sont une condition sine qua non de l'efficacité opérationnelle et de l'autonomie stratégique.

L'une des difficultés majeures réside dans le fait que les spécifications en vigueur dans la sphère militaire reposent encore largement sur des standards anciens, développés dans les années 1990, tels que le Vector Product Format (VPF) ou ses déclinaisons dans la série VMAP. Ces formats historiques, bien que robustes à leur époque, se révèlent aujourd'hui inadaptés face aux exigences contemporaines d'interopérabilités, de gestions de données complexes, et de compatibilités avec les systèmes d'information civils et interalliés. Dans cette perspective, deux standards majeurs émergent comme piliers du futur référentiel : GML (Geography Markup Language) et GeoPackage.

Le standard GML, norme issue de l'ISO et de l'OGC, constitue une référence pour la description des objets géographiques, intégrant les dimensions spatiales, temporelles et topologiques. Toutefois, sa complexité a conduit au développement de profils restreints, tel que le GML simple Feature, spécifiquement adapté aux besoins des échanges opérationnels par sa légèreté et sa simplicité de mise en œuvre. À côté de GML, le format GeoPackage, développé par l'OGC, apparaît comme le candidat le plus pertinent pour la structuration des données vecteurs militaires à moyen terme. Ce format encapsule des données vecteurs et raster dans une base SQLite, optimisée pour des environnements contraints (déconnexion, faible bande passante). Il permet ainsi une diffusion aisée, un stockage efficace, et une intégration facilitée dans les systèmes embarqués. Son adoption par les communautés civiles et militaires (notamment aux États-Unis) renforce son positionnement comme futur standard de référence pour les forces armées.

Cependant, la généralisation de GeoPackage pour la Défense nécessite des adaptations. C'est précisément le rôle des profils normatifs développés au sein du DGIWG, tels que le DGIWG 126 (Profil GeoPackage)[1295], qui intègrent les spécificités propres aux besoins militaires : structuration particulière des jeux de données, prise en charge de la symbologie, gestion avancée des métadonnées, compatibilité avec les modèles sémantiques militaires (DGIF/NGIF), et tuilage multiéchelles pour les grandes quantités de données. La dernière version (1.1) du profil DGIWG a ainsi été publiée le 2 mai 2025 et intègre un profil d'encodage pour les données d'élévation. Ces profils garantissent que les formats employés répondent aux exigences stratégiques des forces armées tout en étant interopérables

[1295] DGIWG 126, DGIWG GeoPackage Profile 1.3.1, 2 mai 2025 https://dgiwg.org/documents/dgiwg-standardsset126.

avec les systèmes civils. De plus, des travaux au sein du programme MGCP visent actuellement à adapter le profil développé par le DGIWG aux besoins du programme de coproduction. Là encore certaines modifications sont nécessaires, afin d'assurer une cohérence entre ce profil et le Feature Catalogue (catalogue d'entités) employé par MGCP. De plus, plusieurs visions d'un profil GeoPackage MGCP s'opposent aujourd'hui au sein du programme. Ainsi, la France et le Canada travaillent tous deux à des règles d'implémentation du profil Geopackage sur des bases différentes, démontrant des approches pas toujours compatibles sur l'emploi possible du format Geopackage pour les besoins du programme.

L'évolution des normes concernant les données vecteur pour la Défense s'inscrit également dans le contexte des programmes capacitaires modernes, tels que GÉODE 4D, qui vise à doter les armées d'une capacité cohérente de production et de diffusion de données géographiques, couvrant toutes les échelles et intégrant des composantes 3D essentielles pour les environnements urbains complexes. Dans ce cadre, des standards complémentaires, tels que CityGML[1296] (pour la modélisation 3D des espaces urbains) et ses déclinaisons modernes, comme CityJSON[1297] jouent un rôle central. Les enjeux sont également institutionnels et internationaux. La coexistence de différentes approches normatives, entre les travaux de l'OGC, ceux du DGIWG, et les exigences propres à l'OTAN (STANAG NGIF), impose une vigilance permanente pour assurer l'alignement des schémas d'application. Le rôle actif joué par certaines nations alliées, en particulier les États-Unis avec leurs profils nationaux et leurs programmes liés au renseignement géospatial, impose aux acteurs nationaux une implication forte dans ces dynamiques pour défendre leurs besoins spécifiques.

Ainsi, la normalisation des données vecteurs pour la Défense ne se réduit pas à un enjeu technique. Elle est l'expression d'une stratégie globale visant à garantir la maîtrise des données géographiques, à préserver l'autonomie décisionnelle des forces armées, et à renforcer leur interopérabilité avec les alliés. Ce processus repose sur une articulation rigoureuse entre veilles technologiques, participation active aux instances de normalisation, et coordination nationale consolidée, afin d'assurer que les formats adoptés, loin d'être de simples outils techniques, deviennent des leviers d'efficacité et de souveraineté.

[1296] OGC City Geography Markup Language (CityGML), 13 septembre 2021. Cette norme définit un modèle conceptuel et un format d'échange pour la représentation, le stockage et l'échange de modèles de villes virtuelles en 3D. Consultable ici: https://www.ogc.org/standards/citygml/.

[1297] CityJSON Community Standard, Ed. 2, 20 novembre 2022. Cette norme communautaire est un format d'échange de données pour les modèles numériques 3D de villes et de paysages. L'encodage JSON de CityJSON met en œuvre un sous-ensemble du modèle de données CityGML (version 3.0) et comprend un mécanisme d'extension spécifique à JSON. Consultable ici: https://www.ogc.org/standards/cityjson/.

3.3 Nouvelle technologie et normalisation militaire de demain

La montée en puissance des services Web dans les infrastructures géospatiales contemporaines constitue l'une des transformations les plus profondes de l'architecture des systèmes d'information géographique. Dans les environnements militaires, cette mutation revêt une importance stratégique, en ce qu'elle conditionne la capacité des forces à accéder en temps réel à des informations géographiques précises, cohérentes, contextualisées, et à les intégrer dans des chaînes décisionnelles complexes. La standardisation des services géospatiaux Web répond à une double nécessité, il s'agit d'une part, de garantir l'interopérabilité technique entre des systèmes hétérogènes (nationaux, alliés, civils, militaires), et d'autre part, d'assurer la pérennité, la sécurité et la cohérence des échanges dans un cadre normatif robuste. Dans ce contexte, la normalisation ne se réduit pas à la définition d'interfaces, mais s'inscrit dans une stratégie systémique, où chaque service est intégré à une architecture modulaire et évolutive.

Les standards historiques de l'OGC, tels que WMS, WFS, WCS, ou CSW, ont été les premières pierres de cette infrastructure. Fondés sur l'architecture OWS (OGC Web Services), ils ont permis l'émergence d'une interopérabilité fonctionnelle, fondée sur des opérations standards (GetMap, GetFeature, GetCoverage, etc.). Néanmoins, les évolutions technologiques, notamment l'usage généralisé d'APIs RESTful, le besoin d'accès asynchrone, la gestion de grands volumes de données temps réel, ont mis en lumière les limites de ce paradigme. En réponse, une nouvelle génération de standards est en cours d'élaboration au sein de l'OGC : les OGC APIs (Features, Tiles, Maps, Records, Coverages, styles, etc.). Ces interfaces, construites sur les principes du Web moderne (OpenAPI, HTTP verbs, JSON), visent à démocratiser l'accès aux services géospatiaux, en les rendant plus accessibles aux développeurs généralistes et plus facilement intégrables dans des écosystèmes cloud ou mobiles. Cette nouvelle approche ne remplace pas immédiatement les standards existants, mais les complète, en visant un socle plus modulaire, plus agile, et orienté vers l'expérience utilisateur.

Pour la communauté de Défense, cette transition vers les APIs constitue un enjeu critique d'adaptation et de souveraineté. Elle implique de redéfinir les profils d'implémentation, de garantir la compatibilité avec les infrastructures existantes, et d'anticiper les ruptures technologiques. Les travaux engagés autour du STANAG 6523[1298], par exemple, témoignent d'un effort de convergence entre les visions portées par l'OGC, le DGIWG et l'OTAN. En parallèle, les exercices d'interopérabilité tels que l'exercice CWIX, et testbeds de l'OGC, constituent des laboratoires d'expérimentation essentiels. Ils

[1298] NATO Defence Geospatial Web Services (AGeoP-26 Ed A Ver 1) 2020. https://nso.nato.int/nso/nsdd/main/standards/stanag-details/8807/EN

permettent de confronter les standards à des conditions opérationnelles, de tester la robustesse des implémentations, et de faire émerger des recommandations pratiques. Ces retours d'expérience viennent enrichir les normes, en assurant une rétroaction constante entre spécification et pratique.

Enfin, la France, par l'intermédiaire de ses institutions techniques, joue un rôle actif dans la structuration de la gouvernance des services géospatiaux de Défense. Elle participe à la définition des profils, à la veille normative, aux groupes de travail sur les APIs émergentes, et à l'harmonisation des spécifications au sein des coalitions internationales. Cette position lui permet de défendre ses intérêts stratégiques, de garantir la compatibilité de ses systèmes avec les standards OTAN et européens, et d'influencer l'évolution des normes vers une vision plus ouverte, plus modulaire, et technologiquement souveraine.

La maîtrise et la standardisation des données géographiques d'imagerie et des données maillées constituent également un enjeu stratégique majeur pour les forces armées contemporaines. Dans un environnement opérationnel où l'information géospatiale conditionne aussi bien la planification tactique que l'anticipation stratégique, l'adoption de formats et normes cohérents devient une nécessité impérieuse. Cet impératif est d'autant plus crucial que les systèmes d'information interconnectés, les capteurs de nouvelle génération et les exigences d'interopérabilité OTAN complexifient le panorama technologique.

L'un des enjeux centraux de cette normalisation réside dans l'intégration maîtrisée des produits d'imagerie (images satellites, photographies aériennes) et des modèles numériques de terrain (MNT) dans les chaînes opérationnelles. La Défense s'oriente vers un socle normatif fondé sur les travaux de l'ISO/TC 211, de l'OGC et du DGIWG, chacun intervenant à des niveaux distincts, mais complémentaires de la chaîne de production, d'encodage et de diffusion de ces données. Parmi les normes majeures en matière d'encodage de données maillées et d'imagerie figure le GMLJP2, format hybride associant compression JPEG 2000 et encapsulation de métadonnées au format GML. Ce format est privilégié pour les données compressées haute résolution utilisée dans les échanges opérationnels, notamment dans les chaînes de renseignement. Son usage est consolidé par des profils spécifiques développés par le DGIWG, assurant l'interopérabilité avec les systèmes militaires alliés. Le format GeoTIFF, quant à lui, demeure la référence pour le stockage de données d'élévation non compressées ou faiblement compressées, utilisé notamment dans les bases de données topographiques ou les modèles numériques de surface. Son adoption est renforcée par des profils OTAN spécifiques, garantissant une compatibilité avec les référentiels géodésiques actualisés. En complément, la norme

JPEG2000, dans ses multiples déclinaisons (partie 1[1299], 2[1300], 15[1301] notamment), permet d'assurer des compressions performantes des images tout en conservant une qualité élevée. Cette capacité est essentielle pour les systèmes contraints par des volumes de données importants, comme ceux intégrés dans les programmes de renseignement image.

En définitive, la normalisation des données d'imagerie et des données maillées pour la Défense repose sur une articulation complexe entre normes internationales civiles, déclinaisons militaires spécifiques, exigences OTAN et besoins propres aux capacités françaises. Ce processus normatif n'est pas seulement technique, il est le socle d'une souveraineté opérationnelle fondée sur une maîtrise complète de l'information géospatiale, garantissant une interopérabilité fiable avec les partenaires tout en préservant l'autonomie stratégique.

L'analyse des mutations technologiques affectant les services géospatiaux Web et les données d'imagerie militaire révèle que la normalisation dans le domaine de la défense constitue aujourd'hui un déterminant stratégique de la souveraineté opérationnelle et de l'autonomie décisionnelle des forces armées. À l'intersection de trois dynamiques convergentes, à la fois modernisation des architectures informationnelles, exigences croissantes d'interopérabilité interalliée et impératif de maîtrise souveraine des données, la France se trouve aujourd'hui confrontée à des choix normatifs dont les implications dépassent largement le périmètre des systèmes d'information géographique pour engager la capacité même des armées à conduire des opérations dans un environnement stratégique en recomposition.

La transition des standards historiques de l'OGC vers les nouvelles OGC APIs illustre les tensions inhérentes à tout processus de modernisation normative dans le contexte militaire. D'un côté, l'adoption d'interfaces RESTful, modulaires et orientées cloud répond à des exigences fonctionnelles incontournables, qu'il s'agisse de la démocratisation de l'accès aux services géospatiaux pour les développeurs, l'intégration facilitée dans les écosystèmes mobiles et déconnectés, ou encore la gestion optimisée des flux massifs de données en temps réel. De l'autre, cette transition impose une refonte profonde des profils d'implémentation, une réévaluation des compatibilités avec les infrastructures existantes et, plus fondamentalement, une vigilance accrue quant à la maîtrise des dépendances technologiques induites. Le programme GEODE 4D, qualifié de *« carte numérique vivante du XXIe siècle »* par ses concepteurs[1302], incarne cette double exigence de modernisation et de souveraineté.

[1299] ISO/IEC 15444-1 : 2024 Technologies de l'information — Système de codage d'images JPEG 2000. Partie 1: Core, Ed. 5, 2024. https://www.iso.org/fr/standard/87632.html

[1300] ISO/IEC 15444-2 : 2023 Technologies de l'information — Système de codage d'images JPEG 2000. Partie 2: Extensions, Ed. 3, 2023. https://www.iso.org/fr/standard/84573.html

[1301] ISO/IEC 15444-15:2019 Information technology — JPEG 2000 image coding system. Part 15: High-Throughput JPEG 2000. https://www.iso.org/standard/76621.html

[1302] IGN / Ministère des Armées, « GÉODE 4D — Présentation du programme, dossier de presse conjoint IGN-DGA », Paris, 2021 ; Ministère des Armées, « communiqué de presse sur le renouvellement du partenariat IGN-Armées », Paris,

Fournir aux forces armées une vision interopérable et cohérente de l'environnement géophysique, conforme au concept OTAN de Recognised Environmental Picture, tout en préservant une chaîne complète d'information géographique maîtrisée de bout en bout. Les travaux engagés autour du STANAG 6523 témoignent des efforts de convergence entre les orientations portées par l'OGC, le DGIWG et l'Agence OTAN des communications et de l'information, malgré des tensions récurrentes sur les profils d'implémentation. Ces divergences, loin d'être anecdotiques, reflètent des conceptions différentes de l'équilibre à trouver entre interopérabilité maximale et préservation de marges d'autonomie nationale. La stratégie de transformation numérique de l'OTAN, adoptée en 2022 et déclinée en 2024 dans une stratégie de mise en œuvre détaillée, place l'interopérabilité numérique au fondement même de la capacité de l'Alliance à conduire des opérations multimilieux[1303]. Cette ambition suppose non seulement une harmonisation des formats de données et des protocoles d'échange, mais également une convergence des architectures, des ontologies et des cadres de gouvernance de la donnée. La stratégie de la donnée pour l'Alliance, publiée en 2025, consacre l'objectif d'un « *écosystème de partage des données à l'échelle de l'Alliance* » fonctionnelle à l'horizon 2030, intégré au moyen d'une dorsale numérique commune et reposant sur des métadonnées standardisées conformément au STANAG 5636[1304].

Pour la France, cette dynamique d'intégration otanienne pose la question des périmètres de souveraineté. Comme le souligne la doctrine du Ministère des Armées, la souveraineté numérique en matière de défense est la condition même de la liberté d'action dans le cyberespace[1305]. Cette exigence se décline en plusieurs dimensions interdépendantes. Tout d'abord, la maîtrise des données sensibles sur des infrastructures contrôlées, la capacité à opérer de manière autonome hors du cadre allié, et la préservation d'une base industrielle et technologique nationale dans le domaine géospatial. Or, la logique d'interopérabilité poussée qui préside à la transformation numérique de l'OTAN tend structurellement à réduire les marges de différenciation technique entre alliés, ce qui crée une tension permanente entre l'impératif de rapidité et d'adaptabilité et celui de l'autonomie stratégique.

La position de la France dans cette géopolitique de la normalisation militaire présente des atouts significatifs, mais également des vulnérabilités. Parmi les atouts, il convient de souligner l'existence en France d'une chaîne géographique militaire complète, de l'acquisition sur le terrain et depuis l'espace jusqu'à la production des données, reposant sur le ministère des Armées et sur un ensemble d'acteurs

2021.

[1303] OTAN, Stratégie de transformation numérique, 2024.

[1304] OTAN, NATO Data Strategy, publié dans le cadre de la *NATO Digital Transformation Implementation Strategy*, ACT Norfolk, 2025 ; voir aussi OTAN, *Summary of NATO's Data Exploitation Framework Policy*, 22 octobre 2021.

[1305] Lemaire Bertrand, « Vincent Tejedor (Ministère des Armées) : « la souveraineté, c'est garder sa liberté d'action », REPUBLK, 8 décembre 2026.

institutionnels et industriels dont l'IGN constitue le partenaire historique. Le renouvellement du partenariat entre l'IGN et le ministère des Armées en 2021, centré sur le programme GEODE 4D, témoigne de la volonté de pérenniser cette capacité souveraine de production de données géographiques de qualité militaire. La participation active de la France aux instances de normalisation lui permet également de défendre ses intérêts stratégiques et d'influencer l'évolution des standards.

Parmi les vulnérabilités, la dépendance croissante aux technologies cloud, aux plateformes d'intelligence artificielle et aux infrastructures de traitement massif de données pose des défis inédits. Le cloud défense, conçu comme le support technologique de l'interconnexion des systèmes déployés en opérations, doit pouvoir fonctionner en environnement dégradé, contesté, voire déconnecté. Autant de contraintes qui entrent en tension avec les modèles économiques et techniques des fournisseurs de cloud dominants, majoritairement américains[1306].

La normalisation des services géospatiaux Web pour la défense se trouve ainsi au cœur d'un triple enjeu géopolitique. Tout d'abord, l'équilibre entre intégration otanienne et autonomie stratégique. La France, qui assumera en 2026 le rôle de nation-cadre de l'Allied Reaction Force, doit démontrer sa capacité à assurer l'interopérabilité technique avec l'ensemble des alliés tout en préservant ses marges de manœuvre pour des opérations nationales ou en coalition ad hoc[1307]. Cette position suppose une maîtrise fine des standards, permettant d'être interconnecté sans dépendre d'autrui. Ensuite, la préservation d'une base industrielle et technologique nationale. Les compétences en normalisation géospatiale constituent en effet un actif stratégique dont la pérennité suppose des investissements soutenus en formation, en veille technologique et en participation aux instances internationales. La désignation d'un conseiller spécial et champion numérique français à l'OTAN témoigne de la reconnaissance de cet enjeu au plus haut niveau. Enfin, l'anticipation des ruptures technologiques. L'émergence de l'intelligence artificielle dans le traitement des données géospatiales, la transition vers les architectures post-quantiques sécurisées, le développement des jumeaux numériques de théâtres d'opérations constituent autant de terrains où se joueront les batailles normatives de demain. La capacité de la France à peser sur ces standards conditionnera sa place dans l'écosystème géospatial militaire du futur.

[1306] Bomont Clotilde., « Le cloud défense : défi opérationnel, impératif stratégique et enjeu de souveraineté », Policy Commons Focus stratégique, n° 107, IFRI, novembre 2021, 64 p.

[1307] Ministère des Armées, « ARF26 EP01 | La France nation-cadre du dispositif de réaction rapide de l'OTAN en 2026 », CND, 7 janvier 2026. https://www.defense.gouv.fr/cnd/actualites/arf26-ep01-france-nation-cadre-du-dispositif-reaction-rapide-lotan-2026. Consulté le 10 février 2026.

Conclusion du Chapitre IX

En définitive, la normalisation des nouvelles technologies géospatiales pour la défense illustre de manière exemplaire l'imbrication entre considérations techniques et enjeux géopolitiques qui traverse l'ensemble de cette thèse. Les choix normatifs opérés aujourd'hui ne sont pas des décisions purement techniques susceptibles d'être déléguées aux seuls experts. Ils engagent des trajectoires de long terme, créent des irréversibilités, structurent des dépendances. La normalisation des données géographiques militaires constitue, au même titre que la normalisation civile analysée dans les chapitres précédents, un terrain de la compétition géopolitique contemporaine, avec cette spécificité que les enjeux de souveraineté y sont directement connectés aux capacités opérationnelles des forces armées et, in fine, à la sécurité nationale. La France dispose des atouts nécessaires pour tenir son rang dans cette compétition normative, qu'il s'agisse de son expertise technique reconnue, de sa chaîne géographique militaire complète, de sa participation active aux instances internationales, ou encore de ses programmes capacitaires ambitieux. Encore faut-il que ces atouts soient mobilisés de manière cohérente, dans le cadre d'une stratégie normative explicite. Cette dernière se doit d'articuler les différents niveaux (national, européen, otanien, international) et les différentes temporalités, celle des urgences opérationnelles en premier lieu, celle du moyen terme programmatique ensuite, et enfin celle du long terme technologique. Et ce, afin de s'assurer que la normalisation des données géographiques ne soit jamais une contrainte subie, mais au contraire, demeure un levier de souveraineté opérationnelle et d'autonomie stratégique pour les armées françaises.

Conclusion de la Partie 3

Cette troisième partie avait pour ambition d'interroger l'avenir de la normalisation des données géographiques numériques à l'aube des bouleversements géopolitiques contemporains. En articulant l'examen des recompositions de puissance affectant le processus normatif international (chapitre VII), l'analyse de l'impact des technologies émergentes (chapitre VIII) et l'exploration des scénarios prospectifs (chapitre IX), cette partie a permis de dégager les trajectoires possibles d'un écosystème normatif en profonde mutation.

Tout d’abord, la montée en puissance de la Chine, matérialisée par l'initiative « China Standards 2035 », traduit une stratégie volontariste visant à faire de la normalisation un instrument de projection de puissance. Simultanément, les inflexions protectionnistes américaines et la menace d'un retrait des États-Unis de l'OTAN font peser un risque considérable sur les logiques d'interopérabilité qui sous-tendent les programmes de normalisation européens. Si l'Union européenne tente de définir une troisième voie fondée sur des standards ouverts mais souverains, illustrée par l'« effet Bruxelles » du RGPD, cette ambition repose sur un paradoxe. L'Europe produit des normes, mais dépend largement des plateformes américaines et des équipements asiatiques pour les mettre en œuvre.

L'intelligence artificielle géospatiale, la blockchain, les jumeaux numériques et la cryptographie post-quantique soulèvent chacune des enjeux de normalisation spécifiques où se jouent des rapports de force majeurs. Une fragmentation par blocs pourrait affecter les formats de données d'entraînement des modèles d'IA, les corpus risquant d'être structurés différemment selon les zones d'influence. Parallèlement, le rôle croissant des consortiums privés dans la définition des standards, soulève des interrogations sur l'accaparement de la normalisation par des intérêts marchands. La bataille entre formats ouverts et propriétaires, notamment entre l'OGC et ESRI, illustre cette tension fondamentale pour l'autonomie des institutions publiques.

Aujourd'hui, trois trajectoires semblent possibles. La première est celle d'une fragmentation normative mondiale conduisant à des écosystèmes incompatibles. Des signes avant-coureurs existent déjà, comme le développement du système de coordonnées propriétaire GCJ-02 par la Chine, ou encore celui du référentiel PZ-90 lié à GLONASS par la Russie. Ces initiatives témoignent d'une volonté de certains États de s'affranchir des référentiels occidentaux, au risque de créer des silos géographiques cloisonnés qui compromettraient l'échange d'informations à l'échelle mondiale.

La deuxième trajectoire est celle d'une convergence multiacteurs préservant l'interopérabilité. Cette voie suppose que les instances existantes, qu'il s'agisse de l'ISO/TC 211, de l'OGC ou du DGIWG, parviennent à maintenir un socle commun de normes ouvertes malgré les tensions géopolitiques. Les programmes de coproduction militaire auxquels la France participe, ainsi que les efforts du CNIG pour harmoniser les pratiques nationales, s'inscrivent dans cette logique de coopération normative.

La troisième trajectoire enfin, est celle de l'émergence de standards privés de facto, portés par les grands acteurs technologiques. L'exemple du format GeoJSON, devenu un standard de fait avant toute reconnaissance institutionnelle, ou la domination des API propriétaires de Google Maps et de Mapbox dans les usages courants, illustrent une dynamique où le marché impose ses normes en amont des processus institutionnels, avec le risque d'une dépendance accrue à l'égard de quelques entreprises américaines.

S'agissant de la défense, la France dispose d'atouts significatifs, mais demeure vulnérable face à la dépendance aux technologies cloud américaines et à l'extraterritorialité du Cloud Act. La normalisation des données géographiques militaires constitue ainsi un terrain de compétition géopolitique où les enjeux de souveraineté sont directement connectés aux capacités opérationnelles des forces armées.

Sur le plan théorique, cette partie a confirmé la pertinence d'une approche géopolitique des espaces normatifs. La diplomatie normative s'affirme comme une composante essentielle des stratégies de puissance contemporaines, servant d'instrument de projection d'influence pour les grandes puissances, de levier de différenciation pour les puissances moyennes, et de terrain de négociation pour les pays en développement. Les programmes spatiaux européens comme IRIS², Galileo, ou MUSIS, témoignent d'une volonté de doter l'Union d'une capacité autonome, mais le manque de formation aux enjeux de la normalisation et l'insuffisance des financements constituent des obstacles qui demeurent à surmonter. Si la France reste un acteur de premier plan dans ce domaine, disposant de nombreux atouts tant sur le plan technologique qu’humain, encore faut-il qu'ils soient mobilisés dans le cadre d'une stratégie normative explicite articulant les niveaux national, européen, otanien et international, pour pouvoir réellement déployer tout leur potentiel.

Conclusion générale

Cette thèse avait pour ambition de démontrer que la standardisation des données géographiques numériques constitue un enjeu de souveraineté pour la France, et d'analyser les modalités selon lesquelles l'État français peut défendre ses intérêts dans un écosystème normatif de plus en plus internationalisé et compétitif. Les développements qui ont précédé permettent de valider cette hypothèse centrale et d'en préciser les contours.

L'analyse a d'abord établi que la normalisation, loin d'être un processus purement technique et apolitique, constitue un « espace normatif » au sens géopolitique du terme. Autrement dit, il s’agit d’un territoire immatériel approprié par des acteurs aux intérêts divergents, traversé par des rivalités de pouvoir, et dont le contrôle engage directement la souveraineté des États. Le parcours historique a montré comment la France s'est inscrite dans cet environnement depuis la création de l'AFNOR en 1926, développant une tradition normative singulière qui articule impulsion étatique et expertise technique. L'examen de l'écosystème international a révélé une architecture institutionnelle complexe où s'imbriquent organisations internationales (ISO/TC 211, OGC), instances européennes (CEN, directive INSPIRE) et structures de défense (DGIWG, OTAN), chacune porteuse de logiques propres, mais interdépendantes. Aujourd’hui, la France y occupe une position significative, mais contestée. En effet, si elle dispose d'atouts historiques, expertise technique reconnue, présence dans les secrétariats de comités stratégiques, tradition d'investissement public dans l'information géographique, elle se trouve confrontée à des difficultés structurelles que sont l'érosion du nombre d'experts, les contraintes budgétaires et la fragmentation de la gouvernance nationale.

Cette recherche a ensuite démontré que les données géographiques numériques ne peuvent plus être appréhendées comme de simples objets techniques neutres. Leur dualité ontologique, à la fois objets du cyberespace et représentations de l'espace physique, en fait des ressources stratégiques dont la maîtrise engage directement la capacité des États à connaître, défendre et administrer leurs territoires. Le conflit ukrainien a offert une démonstration saisissante de cette mutation. Les attaques contre les systèmes GIS Arta et Kropyva ont révélé que l'information géographique numérique était devenue simultanément une arme et une cible. Cette dimension conflictuelle se retrouve à toutes les échelles, depuis l'intégration du cyberespace comme cinquième domaine de conflictualité par l'OTAN jusqu'à la multiplication des attaques visant les collectivités territoriales françaises. L'analyse a également mis en lumière une territorialisation paradoxale du cyberespace. Contrairement aux représentations courantes

qui en font un univers fluide et déterritorialisé, les dispositifs de gouvernance et de défense des données géographiques demeurent profondément ancrés dans des lieux précis. La normalisation occupe dans ce dispositif une place ambivalente, car si les standards de l'OGC et de l'ISO ont permis une interopérabilité sans précédent des systèmes d'information géographique, cette ouverture a mécaniquement accru la surface d'attaque des infrastructures et complexifié leur sécurisation.

Enfin, l'enquête ainsi menée a montré que les recompositions géopolitiques contemporaines affectent directement les processus de normalisation internationale. La montée en puissance de la Chine, matérialisée par l'initiative « China Standards 2035 », traduit une stratégie volontariste visant à faire de la normalisation un instrument de projection de puissance. Simultanément, les fluctuations de la politique américaine et la redéfinition des alliances traditionnelles interrogent la stabilité de l'ordre normatif multilatéral. L'analyse des technologies émergentes a révélé que chacune de ces innovations soulève des enjeux de normalisation spécifiques où se jouent des rapports de force géopolitiques majeurs. Enfin, l'examen des scénarios prospectifs tend à distinguer trois trajectoires possibles : une fragmentation par blocs géopolitiques conduisant à des écosystèmes normatifs incompatibles, une convergence multiacteurs préservant l'interopérabilité mondiale, ou l'émergence de standards privés de facto imposés par les grandes plateformes numériques. Dans chacun de ces scénarios, la capacité de la France et de l'Europe à maintenir leur influence normative constitue un déterminant majeur de leur autonomie stratégique. En effet, il apparaît aujourd’hui fondamental que la puissance publique prenne pleinement conscience du rôle essentiel de la standardisation des données géographiques pour la pérennisation de l’indépendance acquise par la France en matière de contrôle des informations géospatiales. Cet atout entretenu de longue date se doit d’être conservé et protégé, autant pour la préservation de notre indépendance en matière d’aménagement du territoire que pour nos forces armées.

Apports de la recherche

Cette thèse a cherché à apporter plusieurs contributions à la connaissance scientifique des enjeux géopolitiques de la normalisation des données géographiques numériques. Sur le plan théorique, elle a posé comme principe une extension de la géopolitique du cyberespace aux espaces normatifs, conceptualisés comme des territoires immatériels où s'exercent des rivalités de pouvoir. Cette approche permet de saisir les processus de normalisation non pas comme de simples exercices de rationalité technique, mais comme des arènes où se négocient des rapports de force, où se jouent des intérêts économiques et stratégiques, où se projettent des visions du monde. La définition de la souveraineté numérique retenue, articulant contrôle des infrastructures critiques, autonomie technologique et capacité normative, a pour but d’offrir un cadre analytique opératoire pour appréhender les enjeux contemporains de la gouvernance des données géographiques.

Sur le plan empirique, cette recherche a produit une cartographie encore inédite de l'écosystème français et international de la normalisation géospatiale, fondée sur vingt-cinq entretiens semi-directifs et l'observation de plus de cent dix réunions à toutes les échelles de la gouvernance normative. Elle a mis en lumière des dynamiques encore peu étudiées dans la littérature francophone, telles que les stratégies d'influence au sein de l'ISO/TC 211, les tensions entre interopérabilité et sécurité au sein du DGIWG, les rapports de pouvoir structurant la gouvernance nationale au sein du CNIG, ou encore les vulnérabilités spécifiques des infrastructures de données géographiques territoriales.

Sur le plan pratique, cette thèse vise également à formuler plusieurs recommandations à destination des acteurs publics français. Elle vise à souligner la nécessité de renforcer la présence française dans les secrétariats des comités techniques stratégiques, d'investir dans la formation d'une nouvelle génération d'experts en normalisation, de mieux articuler les stratégies civiles et militaires, et de promouvoir une approche européenne coordonnée face à la montée en puissance des acteurs extra-européens. Elle met également en garde contre les risques d'une fragmentation normative mondiale qui priverait la France et l'Europe de leur capacité à peser sur les règles du jeu de l'économie numérique.

Limites de la recherche

Toute recherche comporte des limites et ce travail n’y échappe pas, ce dont son auteur est bien conscient. Ainsi, la dimension comparative internationale de cette recherche mériterait d'être approfondie. Si l'enquête a permis d'observer les dynamiques au sein des instances internationales et de recueillir des informations sur les stratégies déployées par d'autres pays, (Chine, États-Unis, Allemagne, Royaume-Uni, Corée du Sud), elle n'a pas pu inclure d'entretiens systématiques avec des acteurs étrangers hors du cadre des réunions internationales. Cette limitation tient principalement à l’inexpérience de l’auteur au moment de la poursuite des enquêtes au sein des instances internationales. Une lacune qui pourrait être compensé par des recherches renouvelés au sein de ces institutions à l’avenir. Les analyses comparatives présentées s'appuient donc principalement sur la littérature secondaire, les documents stratégiques accessibles et les observations informelles. Une compréhension plus fine des mécanismes décisionnels internes aux délégations chinoise ou américaine, par exemple, aurait permis d'affiner l'analyse des rapports de force contemporains au sein de l'ISO/TC 211 ou de l'OGC.

L'accès aux données sensibles relatives aux vulnérabilités cyber et aux incidents de sécurité a constitué une autre contrainte significative. Les organisations victimes de cyberattaques communiquent rarement de manière transparente sur ces événements, et les données consolidées demeurent souvent classifiées ou confidentielles. L'analyse des enjeux de cybersécurité repose donc principalement sur les sources ouvertes, et sur les témoignages recueillis lors des entretiens, nécessairement partiels et parfois contraints par des obligations de réserve. Les incidents rendus publics ne sont pas nécessairement représentatifs de l'ensemble des menaces pesant sur les infrastructures de données géographiques. La couverture géographique des entretiens territoriaux présente également des lacunes. Si l'enquête a pu inclure un terrain ultramarin avec la Martinique, les autres territoires d'outre-mer, tels que la Guyane, la Réunion, Mayotte, la Nouvelle-Calédonie, ou encore la Polynésie française, n'ont pas fait l'objet d'investigations spécifiques, alors qu'ils présentent des enjeux propres en matière de données géographiques : éloignement des centres de décision métropolitains, contraintes de connectivité, exposition particulière aux risques naturels, et parfois statuts juridiques distincts qui complexifient l'application des cadres normatifs nationaux. De même, certaines régions métropolitaines n'ont pu être couvertes, ce qui limite la représentativité des analyses relatives aux plateformes régionales d'information géographique. L’auteur regrette amèrement ces manques à la couverture géographique du

corpus d’enquête, qui sont liés à un fort taux d’échec dans les tentatives de prise de contacts avec les acteurs du milieu.

La temporalité de la recherche constitue enfin une limite inhérente à tout travail portant sur des dynamiques en évolution rapide comme l’objet de cette thèse. Les travaux de terrain se sont achevés fin 2023, alors que les recompositions géopolitiques analysées se poursuivent à un rythme accéléré. Les changements majeurs de la politique américaine depuis janvier 2025, l'évolution du conflit ukrainien et ses répercussions sur la coopération normative au sein de l'OTAN, les développements fulgurants de l'intelligence artificielle générative et leurs implications pour le traitement des données géospatiales, constituent autant d'événements qui modifient en permanence le paysage de la normalisation internationale. Certaines analyses prospectives devront nécessairement être réévaluées à l'aune des évolutions futures.

Malgré ces limites, l’auteur est confiant concernant le fait que la triangulation des méthodes, liant entretiens semi-directifs, observation participante, analyse documentaire, et la diversité des sources confèrent aux résultats une assise empirique solide. L'ampleur du corpus, malgré ses lacunes, a permis de dégager des régularités et d'identifier des dynamiques structurelles qui dépassent les particularités de tel ou tel acteur ou de telle ou telle situation.

Perspectives de recherche

Les limites identifiées ouvrent autant de perspectives pour des recherches ultérieures susceptibles de prolonger et d'enrichir les résultats de cette thèse. Ainsi, une approche comparative systématique des stratégies normatives des grandes puissances dans le domaine géospatial constituerait un prolongement naturel de ce travail. Une telle recherche pourrait mobiliser des entretiens avec des acteurs chinois, américains, indiens et russes, ainsi qu'une analyse approfondie des documents stratégiques nationaux, pour cartographier avec précision les dynamiques de concurrence et de coopération qui structurent l'écosystème normatif mondial. L'émergence de la Chine comme acteur majeur de la normalisation internationale justifie une attention particulière à la stratégie de Beijing et à ses effets sur les équilibres normatifs internationaux.

L'articulation entre normalisation et cybersécurité des données géographiques ouvre également un champ d'investigation prometteur. Les travaux récents de l'OGC sur les standards de sécurité, les réflexions du DGIWG sur la protection des données géospatiales de défense, et l'émergence de la cryptographie post-quantique appellent une analyse des conditions d'intégration des exigences de sécurité dans les processus de normalisation géospatiale, en identifiant les tensions entre les impératifs d'interopérabilité et de protection. Les dynamiques territoriales de la normalisation des données géographiques mériteraient d'être approfondies, notamment dans les outre-mer français. L'analyse conduite dans cette thèse a révélé une géographie différenciée de la vulnérabilité aux risques cyber et de la capacité à participer aux processus normatifs. Une recherche sur les plateformes régionales d'information géographique, les CRIGEs et les collectivités territoriales permettrait de saisir plus finement les rapports de pouvoir infranationaux et les conditions d'appropriation des standards par les acteurs locaux.

L'impact des technologies émergentes sur la normalisation géospatiale constitue une autre piste que de plus amples recherches pourraient creuser. L'intelligence artificielle, les jumeaux numériques, la blockchain et l'informatique quantique transforment en profondeur les modalités de production, de traitement et de diffusion des données géographiques. Une recherche prospective pourrait analyser les trajectoires normatives envisageables pour chacune de ces technologies, en identifiant les acteurs clés et les rapports de force qui détermineront les standards de demain. Une réflexion plus épistémologique pourrait enfin interroger la place de la géographie et de la géopolitique dans l'étude des processus de normalisation. Les travaux de Frédérick Douzet et Amaël Cattaruzza sur la géopolitique du cyberespace, prolongés par cette thèse vers les espaces normatifs, ouvrent un champ disciplinaire

encore peu exploré. Consolider les fondements théoriques de ce programme de recherche permettrait de dialoguer avec les travaux menés en économie politique, en science politique et en sociologie des sciences et techniques.

Au moment où s'achève ce travail, les données géographiques numériques sont devenues des ressources stratégiques dont la maîtrise conditionne la capacité des États à exercer leur souveraineté à l'ère numérique. L'auteur espère qu'il aura su démontrer que la normalisation de ces données, loin d'être une affaire purement technique réservée aux experts, constitue un terrain de confrontation géopolitique où se jouent des rapports de force entre puissances, entre conceptions de la gouvernance mondiale, entre visions de l'avenir du cyberespace. La France dispose d'atouts considérables pour tenir son rang dans cette compétition. À commencer par une tradition d'excellence en matière d'information géographique incarnée par l'IGN, une présence historique dans les instances internationales de normalisation, un tissu d'expertise technique reconnu, et un ancrage européen qui démultiplie sa capacité d'influence. Mais ces atouts ne sauraient suffire sans une stratégie cohérente et des moyens à la hauteur des enjeux. Le renforcement de la présence française dans les comités techniques stratégiques, l'investissement dans la formation des experts, la meilleure articulation entre les acteurs civils et militaires, et la construction d'une position européenne commune constituent autant de chantiers à poursuivre avec détermination.

La question transversale qui a guidé cette recherche : qui gouverne les données géographiques, pour qui, et à quelles fins ? appelle des réponses qui dépassent le seul cadre technique pour engager des choix politiques fondamentaux sur la souveraineté, l'autonomie des territoires et les conditions de la démocratie à l'ère numérique. Protéger les données géographiques, c'est aussi préserver la capacité des sociétés à se représenter elles-mêmes et à maîtriser la connaissance de leurs territoires. C'est, en définitive, défendre une certaine conception de la souveraineté qui ne se réduit ni au contrôle territorial classique ni à l'autarcie technologique, mais qui s'affirme comme capacité à participer de manière significative à la définition des règles qui structurent l'espace numérique mondial.

Les recompositions géopolitiques en cours, qu'il s'agisse de la montée en puissance de la Chine, des inflexions de la politique américaine, ou encore de l'affirmation d'une autonomie stratégique européenne, redessinent en permanence les contours de cet espace normatif. L'issue de ces transformations n'est pas écrite d'avance. Elle dépendra de la capacité des acteurs, et la France n'y fait pas exception, à anticiper les évolutions technologiques, à forger des alliances pertinentes, à mobiliser les ressources nécessaires et, plus fondamentalement, à comprendre que la normalisation des données

géographiques numériques n'est pas un enjeu parmi d'autres, mais l'un des terrains décisifs où se joue l'avenir de la souveraineté à l'ère numérique.

SOURCES PRIMAIRES

Cet inventaire regroupe les matériaux empiriques et documents mobilisés comme sources primaires dans la thèse (enquête de terrain + corpus documentaire).

I. Enquête de terrain

I.1. Entretiens semi-directifs (mars 2022 – juin 2023)

Liste issue du tableau méthodologique présenté en introduction.

I.2. Observation participante (2022–2023)

Synthèse des instances observées (tableau méthodologique).

II. Textes législatifs, réglementaires et documents institutionnels

II.1. Textes législatifs et réglementaires

Arrêté du 15 février 2012 pris en application du chapitre IV du titre V du livre V du code de l’environnement relatif à l’exécution de travaux à proximité de certains ouvrages souterrains, aériens ou subaquatiques de transport ou de distribution, article 7.

Arrêté du 16 septembre 2003, portant sur les classes de précision applicables aux catégories de travaux topographiques réalisés par l’État, les collectivités locales et leurs établissements publics ou exécutés pour leur compte, JORF n° 252 du 30 octobre 2003, page 18546.

Arrêté du 22 décembre 2015 relatif au contrôle des compétences des personnes intervenant dans les travaux à proximité des réseaux et modifiant divers arrêtés relatifs à l’exécution de travaux à proximité des réseaux.

Arrêté du 9 avril 2021 portant nomination au Conseil national de l'information géographique. Arrêté du 9 avril 2021 portant nomination au Conseil national de l'information géographique, Légifrance. Consulté le 12 août 2025.

Code des relations entre le public et l’administration, Article L300-1, modifié par l’ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l’administration.

Conseil national de l'information géolocalisée (CNIG). Décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géolocalisée, modifié par le décret n° 2022-1204 du 30 août 2022.

Décret n° 2009-697 du 16 juin 2009 relatif à la normalisation.

Décret n° 2011-1241 du 5 octobre 2011 relatif à l'exécution de travaux à proximité de certains ouvrages souterrains, aériens ou subaquatiques de transport ou de distribution. Disponible ici : Décret n° 2011-1241 du 5 octobre 2011 relatif à l'exécution de travaux à proximité de certains ouvrages souterrains, aériens ou subaquatiques de transport ou de distribution – Légifrance. Consulté le 13 juin 2025.

Décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géolocalisée.

Décret n° 2011-1371 du 27 octobre 2011 relatif à l'Institut national de l'information géographique et forestière (IGN), version en vigueur au 12 décembre 2015.

Décret n° 2019-165 du 5 mars 2019 relatif au système national de référence de coordonnées (JORF n° 0056 du 7 mars 2019 texte n° 4) et Décret n° 2006-272 du 3 mars 2006 modifiant le Décret n° 2000-1276 du 26 décembre 2000, portant application de l'article 89 de la Loi n° 95-115 du 4 février 1995 modifiée d'orientation pour l'aménagement et le développement du territoire relatif aux conditions d'exécution et de publication des levés de plans entrepris par les services publics, JORF n° 59 du 10 mars 2006, page 3623.

Décret n° 2021-1473 du 10 novembre 2021.

Décret n° 2021-1473 du 10 novembre 2021, portant modification du décret n° 2009-697 du 16 juin 2009 relatif à la normalisation, article 3.

Décret n° 2021-1473 du 10 novembre 2021 relatif à la normalisation. Journal officiel de la République française, 12 novembre 2021.

Décret n° 2022-1204 du 30 août 2022 modifiant le décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géographique, article 1. Décret n° 2022-1204 du 30 août 2022 modifiant le décret n° 2011-127 du 31 janvier 2011 relatif au Conseil national de l'information géographique – Légifrance. Consulté le 12 août 2025.

Décret n° 2023-1096 du 27 novembre 2023 relatif à l'évaluation et au suivi de l'artificialisation des sols, Article 1.

Décret n° 2023-1259 du 26 décembre 2023 précisant les modalités d'application de la définition de la friche dans le code de l'urbanisme.

Décret n° 2025-782 du 6 août 2025 portant création du Commissariat au numérique de défense, JORF n° 0183 du 8 août 2025.

Décret n° 85-790 du 26 juillet 1985 relatif au rôle et à la composition du Conseil national de l'information géographique.

Directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE).

Directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE). Journal officiel de l'Union européenne, L 108, 25 avril 2007.

Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

Directive (UE) 2019/1024 du parlement européen et du conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte).

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

La Loi de programmation militaire 2024-2030 prévoit une enveloppe de 20 milliards d'euros consacrée au numérique, témoignant de l'importance stratégique accordée à ce domaine. Voir Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030.

La loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (la « loi PACTE ») crée un cadre réglementaire pour les actifs numériques et les jetons, en précisant que celui-ci n'est pas applicable aux instruments financiers prenant la forme de jetons. Https : //www.banque-france.fr/system/files/2023-10/rapport_39_f.pd.

Loi n° 2011-12 du 5 janvier 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne, 6 janvier 2011.

Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

Loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République.

Loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités.

Loi n° 2021-1104 du 22 août 2021 portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets.

Loi n° 46-942 du 7 mai 1946 instituant l'Ordre des géomètres experts.

Ordonnance n° 2010-1232 du 21 octobre 2010 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière d'environnement, 21 octobre 2010.

Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, Bruxelles, 3 juin 2021.

RÈGLEMENT D'EXÉCUTION (UE) 2023/138 de la Commission du 21 décembre 2022 établissant une liste d'ensembles de données de forte valeur spécifiques et les modalités de leur publication et de leur réutilisation (Texte présentant de l'intérêt pour l'EEE).

Règlement du Parlement européen et du Conseil, établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union (règlement pour une Europe interopérable), COM(2022) 720 final, Bruxelles, 18 novembre 2022.

Règlement du parlement européen et du conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), COM (2022) 68 finals, Bruxelles, 23 février 2022.

Règlement intérieur du CEN-CENELEC Partie 1 : 2022 : Organisation et structure. Partie 1D : Exigences applicables aux Membres du CEN et du CENELEC.

Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) n° 1024/2012 (OJ L 295, 21.11.2018), 2 octobre 2018.

Règlement (UE) 2022/1925 du parlement européen et du conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques).

Règlement (UE) 2022/2065 du parlement européen et du conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

Règlement (UE) 2022/868 du parlement européen et du conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données).

Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (Data Act).

Règlement (UE) 2024/903 du Parlement Européen et du Conseil du 13 mars 2024 établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union (règlement pour une Europe interopérable), 2024/903, 22 mars 2024. .Https : //eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32024R0903.

Règlement (UE) du parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Règlement (UE) n ° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n ° 1673/2006/CE du Parlement européen et du Conseil Texte présentant de l'intérêt pour l'EEE https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32012R1025.

Règlement (UE) N°1025/2012 du Parlement européen et du Conseil, du 25 octobre 2012, relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision no 1673/2006/CE du Parlement européen et du Conseil. Disponible ici : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025. Consulté le 15 novembre 2025.

III. Normes et standards

ASTM (American Society for Testing and Materials). Standardization News, n° 26, juin 1998.

CEN-CENELEC, « GUIDE 25 : The concept of Cooperation with European Organizations and other stakeholders », (3), novembre 2021.

DGIWG 114 : DGIWG Metadata Foundation, Ed. 2, 12 juillet 2017.

DGIWG, « DGIWG API Whitepaper », Édition : x.0.3, 5 avril 2024.

DGIWG, « DGIWG GeoPackage Profile », ST-DP-19-005, 22 septembre 2023.

ISO 19115-1 : 2014 Informations géographiques — Métadonnées, Ed. 1, 2014. https://www.iso.org/fr/standard/53798.html.

ISO 19115-2 : 2019 Informations géographiques — Métadonnées. Partie 2 : Extensions pour l'acquisition et le traitement. https://www.iso.org/fr/standard/67039.html

ISO 19115-3 : 2023 Informations géographiques — Métadonnées. Partie 3 : Mise en œuvre par des schémas XML. https://www.iso.org/fr/standard/80874.html.

ISO 19136-1 : 2020. Information géographique — Langage de balisage en géographie (GML). https://www.iso.org/fr/standard/75676.html

ISO 19152-3 : Modèle du domaine de l’administration des terres (LADM) — Partie 3 : Géoréglementation marine.

ISO 19157-1 : 2023 - Information géographique : Qualité des données -Partie 1 : Exigences générales, avril 2023.

ISO 19157-1 : 2023 Informations géographiques — Qualité des données. Partie 1 : Exigences générales, 2023. .https://www.iso.org/fr/standard/78900.html

ISO 19157 : 2013 : Information géographique — Qualité des données, Ed. 1, 2013. https://www.iso.org/fr/standard/32575.html.

ISO 9000 : systèmes de management de la qualité - principes essentiels et vocabulaire.

ISO, « A French university : Encouraging hands-on experience », 2007. https://www.iso.org/sites/materials/initiatives-in-education/education_initiatives-higher-edu/educational_materials-detail-initiatives8111.html?emid=10.

ISO & CEN, « Lignes directrices relatives à la mise en œuvre de l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne) », (7), 2016. . https://boss.cen.eu/media/CEN/ref/va_guidelines_implementation_fr.pdf

ISO/DIS 19157-3 Information géographique — Qualité des données. Partie 3 : Registre des mesures de la qualité des données, en cours de développement.

ISO, « France - Fostering competitive intelligence », 2009. https://www.iso.org/sites/materials/initiatives-in-education/education_initiatives-higher-edu/educational_materials-detail-initiatives6833.html?emid=124.

ISO/IEC 15444-1 : 2024 Technologies de l'information — Système de codage d'images JPEG 2000. Partie 1 : Core, Ed. 5, 2024. https://www.iso.org/fr/standard/87632.html

ISO/IEC 15444-2 : 2023 Technologies de l'information — Système de codage d'images JPEG 2000. Partie 2 : Extensions, Ed. 3, 2023. https://www.iso.org/fr/standard/84573.html.

ISO/IEC 19941 : 2017 – Information technology — Cloud computing — Interoperability and portability.

ISO/IEC 27001 : 2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences, Ed.3, 2022.

ISO/IEC 27001 : 2022 : Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences, Ed.3, 2022. https://www.iso.org/fr/standard/27001

ISO/IEC, « FDIS 23001-17 - Information technology - MPEG système technologies - Part 17 : Carriage of uncompressed video and images in ISO Base Media File Format » (en développement).

ISO/IEC guide 2, Normalisation et activités connexes — Vocabulaire général, 2004.

ISO/TC 211, Geographic information/Geomatics – Business Plan, 2023.

ISO/TS 19158 : 2012 Information géographique — Assurance qualité relative à l'approvisionnement de données, Ed. 1, 2012. . https://www.iso.org/fr/standard/32576.html

Kaibin Bao, Hristo Valev, Wagner Manuela, et Schmeck Hartmut, « A threat analysis of the vehicle-to-grid charging protocol iso 15118 », Computer Science-Research and Development, 33(1) : 3–12, 2018.

Mats Ahlin, « ISO TC 211 Strategic Business Plan 2023 », 8 décembre 2022.

NATO ACT, « 25 Years of CWIX : Largest-Ever Interoperability Exercise Kicks Off », 3 juin 2024.

NATO ACT, « Cooperative Cyber Defence Centre of Excellence : Locked Shields Exercise Showcased the Power of Cooperative Defence », 28 juillet 2024.

NATO, « AgeoP-26 DEFENCE GEOSPATIAL WEB SERVICES », Edition A, Version 1, NATO STANDARDIZATION OFFICE (NSO), mars 2020.

NATO Defence Geospatial Web Services (AGeoP-26 Ed A Ver 1) 2020. https://nso.nato.int/nso/nsdd/main/standards/stanag-details/8807/EN

NATO JFTC, « Coalition Warrior Interoperability Exercise – the Gold Standard for Assuring Digital Interoperability », 20 juin 2025.

NATO, MC 0296/3 – NATO Geospatial Policy, 2011.

NATO, « NATO Allies and partners participate in large-scale cyber defence exercise », 19 avril 2022.

NATO, NATO Geospatial Information Framework, 2018.

NATO - STANAG 7170, Additional Military Layers (AML) – Digital Geospatial Data Products, pp. 7, 22 février 2022. https://standards.globalspec.com/std/14501420/stanag-7170

NATO STANDARD 1059, Code Lettres des Entités géographiques, Ed B, Version 1, 19 février 2004. https://nso.nato.int/nso/nsdd/main/standards/stanag-details/7105/EN

NATO STANDARD AgeoP-08 NATO Geospatial Metadata Profile, Ed B, Version 1, février 2019. https://nso.nato.int/nso/nsdd/main/standards/ap-details/2769/EN

NATO STO, « Interoperability & Networking of Disparate Sensors and Platforms for Tactical ISR Applications conducts successful live experiment », NATO STO News Archive, 3 janvier 2022. https://www.sto.nato.int/_layouts/mobile/dispform.aspx

NF ISO 690, « Information et documentation - Principes directeurs pour la rédaction des références bibliographiques et des citations des ressources d’information », août 2010.

OASIS Standard. Ws-secureconversation 1.4, 2009.

OASIS Standard. Ws-trust 1.4. https://docs. oasis-open. org/ws-sx/ws-trust/

OGC API - Records - Part 1 : Core, 5 février 2025. https://docs.ogc.org/is/20-004r1/20-004r1.html.

OGC Catalogue Services 3.0 - General Model, 12-168r6, 10 juin 2016.. http://docs.opengeospatial.org/is/12-168r6/12-168r6.html

OGC, ISO/TC 211 et L’IHO, « A Guide to the Role of Standards in Geospatial Information Management », New York, NY, août 2021.

OGC, « OGC API - Features - Part 1 : Core », 14 octobre 2019.

OGC, « SWE Implementation Maturity Engineering Report », 2013. https://portal.opengeospatial.org/files/?artifact_id=53823.

OGC Symbology Conceptual Model : Core Part, 18-067r3, 15 octobre 2020. http://www.opengis.net/doc/IS/SymCore/1.0.

OGC Web Services Security, 17-007r1, 2019. https://www.ogc.org/fr/publications/standard/security/.

IV. Rapports institutionnels et documents de stratégie

ANSSI, Panorama de la cybermenace 2024, 2025.

Assemblée Nationale, « Compte rendu Commission de la défense nationale et des forces armées — Audition, à huis clos, de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information. », Compte rendu n° 54, 27 mai 2020.

BASDEVANT Adrien, FRANCOIS Camille, et RONFARD Rémi, « Mission exploratoire sur les métavers », octobre 2022, p. 9. https://www.economie.gouv.fr/files/files/2022/Rapport-interministeriel-metavers.pdf.

BECHT Olivier et GASSILOUD Thomas, « Rapport d'Information déposé par la Commission de la Défense Nationale et des Forces Armées en conclusion des travaux d'une mission d'information sur les enjeux de la numérisation des armées », Assemblée Nationale, 30 mai 2018. https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b0996_rapport-information. Consulté le 22 mai 2025.

BERMANN Sylvie, et FABRY Elvire, « Construire l'autonomie stratégique de l'Europe face à la Chine », Institut Jacques Delors, rapport n° 124, décembre 2021, p. 12. .Https : //institutdelors.eu/wp-content/uploads/2021/12/R124_Construire_autonomie_Europe_face_Chine_Interactif.pdf.

CAPO-CANELLAS Vincent, « Acteur de référence de la donnée géolocalisée souveraine, l'IGN avance sur un chemin à baliser », Rapport d'information n° 17 (2022-2023), déposé le 5 octobre 2022, p.7. https://www.senat.fr/rap/r22-017/r22-0170.html.

CAPO-CANELLAS Vincent, « Rapport d'information fait au nom de la commission des finances sur l'Institut national de l'information géographique et forestières (IGN) », n° 17, Sénat, 5 octobre 2022.

Champeau Guillaume, « Le Sénat exclut les normes AFNOR de l'Open Data », Numerama, 27 avril 2016.

CJUE, Data Protection Commissioner c. Facebook Ireland Ltd et Maximillian Schrems, aff. C-311/18, 16 juillet 2020.

CMA CGM, « RAPPORT RSE 2023 : Déclaration de performance extra-financière », p. 38, 2023. https://www.cmacgm-group.com/api/sites/default/files/2024-02/CMA%20CGM_Rapport%20RSE%202023_Web%20(1).pdf.

CNIL, « La Plateforme des données de santé (Health Data Hub) », 11 juin 2020.

ANSSI / CERT-FR, « Collectivités territoriales - Synthèse de la menace », Rapport menaces et incidents du CERT-FR, réf. CERTFR-2025-CTI-002, 24 février 2025. https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-002.

Commission de la défense nationale et des forces armées, « La préparation à la haute intensité », Rapport d'information n° 5054, Assemblée nationale, 17 février 2022, 187 pages, p. 22.

Commission européenne. « Staff Working Document on common European data spaces« , 45 final, janvier 2024.

Commission européenne. « Common European data spaces« , Shaping Europe's digital future, 2024

Commission européenne, « When open data meets data spaces« , data.europa.eu, 2024.

« Common European Data Spaces », 10 octobre 2024. https://digital-strategy.ec.europa.eu/en/policies/data-spaces

Commission européenne, Façonner l'avenir numérique de l'Europe, COM(2020) 67 final, 19 février 2020, p. 2.

Commission Européenne, « Initiative relative à l'infrastructure européenne de communication quantique (EuroQCI) », juin 2019. . Consulté le 21 janvier 2023.https://digital-strategy.ec.europa.eu/fr/policies/european-quantum-communication-infrastructure-euroqci.

Commission Européenne, « RECOMMANDATION de la Commission du 11.4.2024 relative à une feuille de route pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique », Bruxelles, le 11 mars 2024, C(2024) 2393 final. . Consulté le 22 mai 2024. https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.

Commission européenne, « Commission Staff Working Document on Common European Data Spaces », doc. SWD 21 final, Bruxelles, 24 janvier 2024. https://digital-strategy.ec.europa.eu/fr/library/commission-staff-working-document-common-european-data-spaces.

Communication de la commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions, Cadre d'interopérabilité européen – Stratégie de mise en œuvre (COM [2017] 134 finals), Bruxelles, 23 mars 2017.

Communication de la Commission européenne de la Commission au parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Une stratégie européenne pour les données », Bruxelles (COM(2020) 66 final), 19 février 2020.

Conseil d'État, 1ère - 6ème chambres réunies, 13/04/2016, 389798, Publié au recueil Lebon. Https : //www.legifrance.gouv.fr/ceta/id/CETATEXT000032405469/. Consulté le 3 mai 2024.

Conseil d'État de la République populaire de Chine, « Approfondissement du plan de réforme du travail de normalisation » (深化标准化工作改革方案), 11 mars 2015. Disponible ici : www.gov.cn.

Conseil d'État, ord. réf., 21 septembre 2020, n° 444514.

Consulté le 7 janvier 2023, p. 3. Communication From The Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, « An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market », Brussels, 2.2.2022, COM(2022) 31 final, p. 3. https://ec.europa.eu/docsroom/documents/48598.

Cour des Comptes, « La loi de Programmation Militaire (LPM) 2019 – 2025 et les Capacités des Armées », Rapport Publique Thématique, mai 2022, p. 57. https://www.ccomptes.fr/system/files/2022-05/20220511-rapport-bilan-loi-programmation-militaire.pdf. Consulté le 18 juin 2025.

De GANAY Claude et GOUTTEFARDE Fabien. « Rapport d'information de la Commission de la défense et des forces armées de l'Assemblée nationale sur les systèmes d'armes létaux autonomes », n° 3248, 22 juillet 2020.

DÉCISION D'EXÉCUTION (UE) 2024/459 de la Commission du 1er février 2024, sur la création du consortium pour une infrastructure numérique européenne intitulé « Networked Local Digital Twins towards the CitiVERSE » (EDIC LDT CitiVERSE). https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202400459.

Defence Geospatial Information Working Group (DGIWG), fondé en 1983.

Document de travail des services de la Commission, « résumé de l'évaluation de La DIRECTIVE 2007/2/EC établissant une infrastructure d'information spatiale dans la Communauté européenne (INSPIRE). », Bruxelles, 13 juillet 2022.

Document de travail des services de la Commission résumée de l'évaluation de, La DIRECTIVE 2007/2/EC établissant une infrastructure d'information spatiale dans la Communauté européenne (INSPIRE)., Bruxelles, 13 juillet 2022.

Commission européenne, « European Blockchain Services Infrastructure », digital-strategy.ec.europa.eu, 25 octobre 2024. https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure.

European Commission, « SMEs and standardisation in Europe », EIM Business & Policy Research, Zoetermeer, Octobre 2006. file : ///C : /Users/remki/Downloads/smes_and_standardisation_in_europe_6_11_2006_3835.pdf.

FANTIN, S., « Data Protection Commissioner v Facebook Ireland Limited », Maximillian Schrems : AG discusses the validity of standard contractual clauses and raises concerns over privacy shield (C-311/18 Schrems II, Opinion of AG Saugmandsgaard Øe), European Data Protection Law Review, n°6, 2020, pp. 325–331 https://edpl.lexxion.eu/article/EDPL/2020/2/21.

FAUCHIER-MAGNAN Emilie (IGAS) et Fradel Julien (Conseil d'État) (rapporteurs), « Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé », Rapport au Conseil d'État, 5 décembre 2023.

FAURE-MUNTIAN Valéria, Rapport d'information sur les données géographiques souveraines, Assemblée nationale, n° 1178, 17 juillet 2018.

FAURE-MUNTIAN Valéria, « Les données géographiques souveraines », Rapport au gouvernement, juillet 2018, p. 31. Rapport_DonneesGeographiquesSouveraines.pdf. Consulté le 12 septembre 2025.

Federal Bureau of Investigation (FBI), China's Standards Strategy: A Guide to Beijing's Technology Ambitions, Liaison Intelligence Report n° 210303004, Washington D.C., 3 mars 2021.

GAUGITSCH Roland et al., « Integration of Geographic and Statistical data for better EU policy making », Commission for Territorial Cohesion Policy and EU Budget, 2021.

Groupe AFNOR, « Rapport d'activité et de responsabilité sociétale 2022 », 2023.

Cybermalveillance.gouv.fr et CNIL, « Guide obligations et responsabilités des collectivités locales en matière de cybersécurité », juillet 2021. https://www.cybermalveillance.gouv.fr/medias/2022/07/220630_FranceRelance_Guide-1-1.pdf.

HENNION Christine, ALTOUNIAN Magali et MONTHUBERT Bertrand, « Rapport de la Mission Data et Territoires », Ministère de la Transformation et de la Fonction Publique, septembre 2023, p. 5.

HUGON Philippe et coll., « Rapport d'analyse comparative des processus d'intégration économique régionale, Paris, Ministère français des affaires étrangères », 2001, p. 8.

IGN, « Jumeau numérique de la France et des territoires : Dossier de candidature à France 2030 », p. 10, novembre 2024.

Commission européenne, « Implementing Regulation on the adoption of a European Common Criteria-based cybersecurity certification scheme », 31 janvier 2024. https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-adoption-european-common-criteria-based-cybersecurity-certification-scheme.

Commission européenne, « Infrastructure européenne de services Blockchain », digital-strategy.ec.europa.eu, 25 octobre 2024. https://digital-strategy.ec.europa.eu/fr/policies/european-blockchain-services-infrastructure.

Commission européenne, « Joint Initiative on Standardisation under the Single Market Strategy », Bruxelles, 20 août 2018.

Ministère de l'Économie et des Finances / Direction Générale des Entreprises (DGE), « Journée d'information MIE numérique », 11 décembre 2024. https://www.entreprises.gouv.fr/files/files/Evenements/2024/Info%20Day%20-%20CEF%20Digital_PPT%20Presentation_Final_FR.pdf.

LAMURE Élisabeth, « Où va la normalisation ? - En quête d'une stratégie de compétitivité respectueuse de l'intérêt général », Rapport d'information fait au nom de la commission des affaires économiques sur l'impact de la normalisation, Sénat (n° 627), 12 juillet 2017.

La Commission européenne, « Une stratégie de l'UE en matière de normalisation. Définir des normes mondiales à l'appui d'un marché unique européen résilient, vert et numérique », Bruxelles, 2 février 2022.

Liste complète disponible dans Commission européenne. « Second Staff Working Document on Data Spaces« , SWD, janvier 2024.

LYDIE Evrard, « Politique nationale de normalisation et stratégie pour la compétitivité de notre économie », Rapport remis au ministre de l'Économie, de l'Industrie et du numérique, décembre 2014.

Ministère de l'Europe et des Affaires étrangères, « Ambassadeur pour le numérique : Synthèse du rapport d'activité 2020 », 2020. https://www.diplomatie.gouv.fr/IMG/pdf/synthese_fr_rapport_d_activite_ambassadeur_pour_le_numerique_2020_cle068aba.pdf.

Ministère de l'Intérieur, « Livre blanc de la sécurité intérieure », p. 233, 2020.

Ministère de la Transformation et de la Fonction publiques, « Rapport de la mission Data et territoires », septembre 2023, p. 30. https://www.vie-publique.fr/files/rapport/pdf/291763.pdf. Consulté le 23 mars 2025.

Rapport de la Commission au Parlement européen, au Conseil et au Comité économique et social européen, « Rapport sur les conséquences de l'intelligence artificielle, de l'Internet des objets et de la robotique sur la sécurité et la responsabilité (COM(2020) 64 final) », Bruxelles, 19 février 2020.

Rapport du 117e Congrès des notaires de France, « Les premières expériences de registre immobilier en blockchain », 31 janvier 2021. https://www.rapport-congresdesnotaires.fr/2021-rapport-du-117e-congres/les-premieres-experiences-de-registre-immobilier-en-blockchain.

Rapport sur la politique publique de la donnée, des algorithmes et des codes sources, 23 décembre 2020. https://www.info.gouv.fr/actualite/remise-du-rapport-sur-la-politique-publique-de-la-donnee-des-algorithmes-et-des-codes-sources.

QUERET Sophia, « Rapport de la Commission AFNOR/CN INFO GÉO - Information géographique et systèmes géodésiques - juillet 2023 - septembre 2024 », 2023.

Commission européenne, « Stratégie Blockchain et Web3 », digital-strategy.ec.europa.eu, 12 décembre 2024. https://digital-strategy.ec.europa.eu/fr/policies/blockchain-strategy.

United Nations Economic Commission for Africa, « Africa must harness geospatial technology for sustainable development », 10 octobre 2023. . Consulté le 18 novembre 2025. https://www.uneca.org/stories/africa-must-harness-geospatial-technology-for-sustainable-development.

United Nations Economic Commission for Africa (ECA), « Developing a Regional Spatial Data Infrastructure in Africa », 2018.

URVOAS Jean-Jacques et VERCHERE Patrice, « Rapport d'information par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement », Assemblée nationale (n° 1022), 14 mai 2013.

IV.1. Documents techniques et working papers

ALDAZ-CARROLL, E., « Regional Approaches to Better Standards Systems », World Bank Policy Research Working Paper 3948, 2006, p. 9.

MARTINOVIC, I., KELLO, L., SLUGANOVIC, I., « Blockchains for Governmental Services : Design Principles, Applications, and Case Studies », Center for technology and Global Affairs, Working Paper Serie n°7, décembre 2017. https://www.ctga.ox.ac.uk/sites/default/files/ctga/documents/media/wp7_martinovickellosluganovic.pdf.

BARON Justus et coll., « Making the Rules : The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights », TILEC Discussion Paper, Tilburg University, octobre 2019.

MATHEUS Andreas, « Testbed-12 ows common security extension er. Technical report », Open Geospatial Consortium, 2016.

OGC, « Geospatial Standardization of Distributed Ledger Technologies », OGC Discussion Paper, 6 juillet 2018. https://docs.ogc.org/dp/18-041r1/18-041r1.html

SARAFINOF Dimitri, SERVANT Fabrice, RÖNSDORF Carsten et al., « Urban Digital Twins : Integrating Infrastructure, natural environment and people », OGC Discussion paper, p. 10, 2024. #. Consulté le 12 mars 2025. https://docs.ogc.org/dp/24-025.html.

IV.2. Ressources web institutionnelles

2025 Meeting of the International Advisory Committee (IAC) of the UN-GGKIC », Concept Note, 17 avril 2025. . Consulté le 3 octobre 2025. https://ggim.un.org/meetings/2025/2025_Meeting_UN_GGKIC_IAC/.

American National standard for Financial Services, « Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry », ANSI X9.98-2010, 2 février 2017. . Consulté le 21 mars 2024. https://webstore.ansi.org/standards/ascx9/ANSIX9982010R2017.

ANSSI, « Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory », ANSSI-PB-090, 28 janvier 2022. https://cyber.gouv.fr/sites/default/files/2022/01/anssi-guide-recommandations_securite_journalisation_systemes_microsoft_windows_environnement_active_directory.pdf.

ANSSI, « ANSSI views on the Post-Quantum Cryptography transition », cyber.gouv.fr, 21 décembre 2023. https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf.

Archives du ministère des Armées, « La blockchain pour appuyer les projets innovants de l'Armée de Terre – le cas de FIBR2EO », 22 juin 2021. https://archives.defense.gouv.fr/terre/pole-numerique-et-innovation/le-numerique/les-projets-numeriques/la-blockchain-pour-appuyer-les-projets-innovants-de-l-armee-de-terre-le-cas-de-fibr2eo.html

Boyer Claire, « ETSI TC Cyber releases Report on Quantum-Safe Virtual Private Networks », Sophia Antipolis, France, 16 octobre 2018. . Consulté le 10 mai 2025. https://www.etsi.org/committee?id=1382

Boyer Nathalie, « Artist, première expérimentation de la bulle opérationnelle aéroterrestre », DGA, 26 juin 2010. https://archives.defense.gouv.fr/dga/actualite-dga/2009/artist-premiere-experimentation-de-la-bulle-operationnelle-aeroterrestre.html?

BSI - Federal Office for Information Security, « Securing Tomorrow, Today : Transitioning to Post-Quantum Cryptography », 27 novembre 2024. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?

BSI - Fédéral Office for Information Security, « Securing Tomorrow, Today : Transitioning to PostQuantum Cryptography », 27 novembre 2024. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf

Chester Simon, « Le métavers est géospatial », OGC, article de blog, 3 mai 2022. #. Consulté le 24 novembre 2024. https://www.ogc.org/fr/blog-article/the-metaverse-is-geospatial/.

CityJSON Community Standard, Ed. 2, 20 novembre 2022. Consultable ici : https://www.ogc.org/standards/cityjson/.

Conseil National de l'Information géoréférencée (CNIG), « Quadogéo », 28 mai 2025. https://cnig.gouv.fr/gt-quadogeo-a18183.html.

Enisa, « Post-Quantum Cryptography – Integration study », octobre 2022, p.4. . Consulté le 1er avril 2024. https://www.enisa.europa.eu/sites/default/files/publications/Post%20Quantum%20Cryptography-%20Integration%20Publication.pdf

ETSI, « ETSI launches new standard for Quantum-Safe Hybrid Key Exchanges to secure future post-quantum encryption », Sophia Antipolis, France, 25 mars 2025. #. Consulté le 10 mai 2025. https://www.etsi.org/newsroom/press-releases/2513-etsi-launches-new-standard-for-quantum-safe-hybrid-key-exchanges-to-secure-future-post-quantum-encryption.

Géoservices, « Retour sur l'appel à communs pour la conception du Jumeau numérique de la France et de ses territoires », 29 novembre 2024. https://geoservices.ign.fr/actualites/2024-11-jumeaux-numeriques.

Groupe de travail ISO/IEC JTC 1/SC 42 Intelligences artificielles. https://www.iso.org/fr/committee/6794475.html.

High-Level Forum on European Standardisation, « WORKSTREAM 3 NSBs peer-review (including SMEs and civil society inclusiveness) – REPORT Summary of findings from the questionnaires and interviews », septembre 2024. p. 13. https://ec.europa.eu/docsroom/documents/61814.

IGN, « L'IGN finalise son choix de partenaires techniques pour le développement et l'exploitation de la Géoplateforme », 27 janvier 2022. https://www.ign.fr/espace-presse/lign-finalise-son-choix-de-partenaires-techniques-pour-la-geoplateforme.

Information Technology Laboratory Computer Security Division, « Post-Quantum Cryptography Standardization - Post-Quantum Cryptography », CSRC — NIST, 3 janvier 2017. . Consulté le 13 mars 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

Institut Ign, « Des données et logiciels ouverts au service de la Nation ». https://www.ign.fr/institut/des-donnees-et-logiciels-ouverts-au-service-de-la-nation. Consulté le 23 mars 2023.

ISO, « Déclaration de Londres : l'ISO s'engage à agir en faveur du climat », 24 septembre 2021. . Consulté le 12 janvier 2025. https://www.iso.org/fr/news/ref2726.html.

ISO/IEC 14888-4 : 2024 Sécurités de l'information — Signatures numériques avec appendice. Partie 4 : Mécanismes basés sur le hachage à état. https://www.iso.org/fr/standard/80492.html.

ISO/IEC 15444-15 : 2019 Information technology — JPEG 2000 image coding system. Part 15 : High-Throughput JPEG 2000. https://www.iso.org/standard/76621.html.

ISO/IEC 18033-2 : 2006 Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement. Partie 2 : Chiffres asymétriques. https://www.iso.org/fr/standard/37971.html.

ISO/IEC 23837-1 : 2023 Information security — Security requirements, test and evaluation methods for quantum key distribution. Part 1 : Requirements. https://www.iso.org/standard/77097.html.

ISO, « ISO's Action Plan for developing countries 2021-2025 Designed with members, for members. », 10 mai 2021. . Consulté le 10 novembre 2022. https://www.iso.org/news/ref2667.html.

ISO/TC 307 – Blockchain and distributed ledger technologies. https://www.iso.org/committee/6266604.html.

LAMBOIS Marie et DROUADAINE Clément, « Les services Web de l'OGC : Principe et standards », 1er octobre 2018. https://eden.ign.fr/wp-content/uploads/ISN-18.097-Webservices-partie-1.pdf.

Liste des actions prises par les ministères dans le cadre des feuilles de routes ministérielles, 27 avril 2021. https://www.data.gouv.fr/fr/datasets/liste-des-actions-prises-par-les-ministeres-dans-le-cadre-des-feuilles-de-routes-ministerielles/.

Mag Ign, « Géonumérique, la filière qui valait 10 milliards », 30 septembre 2024. https://www.ign.fr/mag/geonumerique-la-filiere-qui-valait-10-milliards. Consulté le 3 mars 2025.

Ministère de l'Économie, « Mise en place du dispositif IA-Cluster pour soutenir l'intelligence artificielle », Direction Générale des Entreprises, 16 juin 2023. . Consulté le 10 décembre 2024. https://www.entreprises.gouv.fr/la-dge/actualites/mise-en-place-du-dispositif-ia-cluster-pour-soutenir-lintelligence-artificielle.

Ministère des Armées, « Présentation du Commissariat au Numérique de Défense », defense.gouv.fr, consulté le 22 janvier 2026. URL : https://www.defense.gouv.fr/cnd/mieux-nous-connaitre/presentation-du-commissariat-au-numerique-defense.

Moody Dustin, « NIST POST-QUANTUM CRYPTOGRAPHY UPDATÉ », National Institute of Standards and Technbology. Mars 2025. #. Consulté le 10 mars 2025. https://csrc.nist.gov/csrc/media/Presentations/2023/nist-post-quantum-cryptography-update/2a-Moody_NIST_PQC_2.pdf.

NATO, « NATO acquires AI-enabled Warfighting System », 14 avril 2025. https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system-.

NATO, « Summary of NATO's Quantum Technologies Strategy », 16 janvier 2024. . https://www.nato.int/cps/en/natohq/official_texts_221777.htmConsulté le 2 septembre 2024.

NIST, « Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process », NIST IR 8413, juillet 2022. . Consulté le 3 janvier 2025. https://csrc.nist.gov/pubs/ir/8413/upd1/final.

OGC, « OGC announces the creation of a new Domain Working Group for Blockchain and Distributed Ledger Technologies », 10 juillet 2019. https://www.ogc.org/announcement/ogc-announces-the-creation-of-a-new-domain-working-group-for-blockchain-and-distributed-ledger-technologies/.

OGC, OGC KML 2.3, 4 août 2015. . https://www.ogc.org/standards/kml/.

OGC, OGC Network Common data Form (NetCDF) Core Encoding Standard version 1.0., 4 mai 2011. https://www.ogc.org/standards/netcdf/.

OMC, « Accord sur l'application des mesures sanitaires et phytosanitaires (Accord SPS) », Division du commerce et de l'environnement, 1er janvier 1995. . Consulté le 21 février 2025. https://www.wto.org/french/tratop_f/sps_f/spsagr_f.htm.

Open Geospatial Consortium, « OGC Augmented Reality Markup Language 2.0 (ARML 2.0) », OGC12-- 132r4, version 1, 24 février 2015. . https://www.ogc.org/standards/arml/Consulté le 6 janvier 2025.

OTAN, « Summary of NATO's Data Exploitation Framework Policy », 22 octobre 2021. . Consulté le 16 juillet 2023. https://www.nato.int/cps/en/natohq/official_texts_210002.html.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32023R1114.

OMC (Organisation mondiale du commerce), « Série des Accords de l'OMC : Obstacles techniques au commerce », Division du commerce et de l'environnement, 1er janvier 1995. https://www.wto.org/french/res_f/booksp_f/tbt3rd_f.pdf.

NIST (National Institute of Standards and Technology), « Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process », NIST IR 8545, mars 2025. https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf.

OTAN (NATO), « Technologies émergentes et technologies de rupture », nato.int, 31 mai 2024. https://www.nato.int/cps/en/natohq/topics_184303.htm.

UN GGIM, « A Guide to the Role of Standards in Geospatial Information Management », février 2022. . https://ggim.un.org/Revised-Standards-Guide/.

UN-GGIM Decision 12/101, établissement du Centre mondial de connaissances et d'innovation géospatiales des Nations unies (UN-GGKIC) à Deqing, Chine. . Consulté le 30 septembre 2025. https://ggim.un.org/meetings/2024/2024_Meeting_UN_GGKIC_IAC/.

IGN, « Une carte d'occupation du sol pour faciliter le suivi de l'artificialisation », ign.fr, 27 mars 2025. https://www.ign.fr/institut/une-carte-doccupation-du-sol-pour-faciliter-le-suivi-de-lartificialisation.

IGN, « Une carte d'occupation du sol pour faciliter le suivi de l'artificialisation », ign.fr, 4 avril 2024. https://www.ign.fr/institut/une-carte-doccupation-du-sol-pour-faciliter-le-suivi-de-lartificialisation.

Union Européenne, « Minimal Interoperability Mechanisms : Advancing Europe’s digital future », 26 août 2024. https://data.europa.eu/en/news-events/news/minimal-interoperability-mechanisms-advancing-europes-digital-future.

US Department of Defense, « Department of Defense Strategy for Operating in Cyberspace », juin 2011. https://csrc.nist.gov/presentations/2011/department-of-defense-strategy-for-operating-in-cy.

VOAS Jeffrey (NIST), Peter Mell (NIST), Phillip Laplante (NIST), et Vartan Piroumian, « Security and Trust Considerations for Digital Twin Technology », NIST, IR 8356, février 2025, p. 5. . Consulté le 19 mars 2025.https://csrc.nist.gov/pubs/ir/8356/final.

World Bank Group, « Cryptocurrencies and Blockchain Europe and Central Asia Economic Update », office of the chief Economist, mai 2018. https://openknowledge.worldbank.org/server/api/core/bitstreams/9be74ccf-8280-571a-a3ee-d4daa12fb10a/content.

BIBLIOGRAPHIE

1Spatial, « Le petit livre de la Gestion des données Géospatiales », 2021. https://1spatial.com/media/roolaoot/006931_1spatial_little-book-data-management_a5_v5_1-4-fr-single-pages.pdf.

ABBAS Nacira, David Jérôme, Napoli Amedeo, « Linkex : A Tool for Link Key Discovery Based on Pattern Structures », ICFCA 2019 - workshop on Applications and tools of formal concept analysis, Frankfurt, Germany. Pp. 33-38, juin 2019.

ADLEMAN, L., « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems », Communications of the ACM, n°21(2), pp. 120 – 126, février 1978. https://dl.acm.org/doi/10.1145/359340.359342.

AFIGÉO, « Les plateformes territoriales de données géographiques : état des lieux, enjeux et perspectives », juin 2023, p. 9.

AFIGÉO, « Les plateformes territoriales de données géographiques, état des lieux, enjeux et perspectives », p. 9, juin 2023.

AFNOR, Communiqué de presse, « Olivier Peyrat, directeur général d'AFNOR, est nommé vice-président « elect » en charge des questions politiques du Comité européen de normalisation (CEN) », 21 juin 2021.

AFNOR, « Baromètre international 2021 », 2021.

AFNOR, « Baromètre international 2023 », Saint-Denis-la-Plaine, AFNOR, 2023. Disponible sur : https://normalisation.afnor.org/actualites/barometre-international-normalisation-2023/

AGGARWAL Sachin, « Treasure of the commons : Global leadership through health data », Centre for International Governance Innovation, 2018. https://www.cigionline.org/articles/treasure-commons-global-leadership-through-health-data/

Agrawal, S. et Gupta, R. D., « Web GIS and its architecture : a review. », Arabian Journal of Geosciences, 10, 518, 2017.

Airbus DS Geo GmbH, « « EULA« DEM Data Alliance Nation », 2016.

AKERLOF George A., « The Market for 'Lemons' : Quality Uncertainty and the Market Mechanism », The Quarterly Journal of Economics, vol. 84, n° 3, 1970, pp. 488-500.

AKERLOF George, « The Market for "Lemmons" : Quality Uncertainty and the Market Mechanism », Quarterly Journal of Economics, n° 84, p. 488 – 500, 1970.

ALVAREZ Leon, Luis F., et Quinn, Sterling, « The value of crowdsourced street-level imagery : Examining the shifting property regimes of OpenStreetCam and Mapillary. », GeoJournal, n° 84, 2019, pp. 395–414.

American National Standards Institute (ANSI), « Understanding the U.S. Voluntary Consensus Standardization and Conformity Assessment Infrastructure », 2020. https://www.standardsportal.org/usa_en/standards_system.aspx.

ANASSE Boutayeb, Lahsen-Chérif Iyad et El Khadimi Ahmed, « A comprehensive GeoAI review: Progress, challenges and outlook », Computers and Geosciences, 2024.

BRADFORD Anu, The Brussels Effect: How the European Union Rules the World, Oxford, Oxford University Press, 2020, p.2.

ARCEP / CREDOC, Baromètre du numérique — Édition 2022, Paris, ARCEP, 2023.

ARMELLE Verdier « L'information géospatiale légale : (1/2) 1. Synthèse des contributions », Afigéo, p. 1, juillet 2019.

Army Recognition, « GPS Jamming key of Russian operational capacities in Ukraine », 2024.

Army Technology, « Radars, reconnaissance and software are shaping the artillery war in Ukraine », 10 juin 2022 : « multiple failed attempts were made to hack this program both during the Donbas conflict and after the 2022 invasion ».

ARON Raymond, « Qu'est-ce qu'une théorie des relations internationales ? », Revue française de science politique, n° 5, 1967, p. 837 – 861.

ARRÊT de la Cour Administrative d'Appel de Lyon, Req. n° 11LY01784, 5 avril 2012.

ARRÊT de la Cour de justice (troisième chambre) du 27 octobre 2016, C-613/14, ECLI : EU : C : 2016 : 821.

ARTHUR W. Brian, « Competing Technologies, Increasing Returns, and Lock-In by Historical Events », The Economic Journal, vol. 99, n° 394, 1989, pp. 116-131.

ARTICLES L. 554-1 à 5 et R. 554-1 à 38 du code de l'environnement, Arrêté modifié du 15 février 2012 pris en application du chapitre IV du titre V du livre V du code de l'environnement relatif à l'exécution de travaux à proximité de certains ouvrages souterrains, aériens ou subaquatiques de transport ou de distribution.

ARUNDEL Samantha, Li Wenwen et Campbell B. Bryan, « Reimagining standardization and geospatial interoperability in today's world », International Journal of Geographical Information Science, 2023.

Asia Society Policy Institute, « Stacking the Deck : China's Influence in International Technology Standards Setting », novembre 2021.

ASHOK Kumar, « India’s Own 5G Technology – 5Gi », National Telecommunications Institute for Policy Research, Innovations & Training (NTIPRIT), 2015. https://ntiprit.gov.in/pdf/gsm2g/All_about_Indias_own_5G_called_5Gi.pdf

ASHTON Philippe, Weber, Rachel, et Zook, Matthew, « The cloud, the crowd, and the city : How new data practices reconfigure urban governance? », Big Data & Society, n° 4, 2017. https://journals.sagepub.com/doi/full/10.1177/2053951717706718.

Associated Press News, « Sweden updates its Cold War-era preparedness booklet », 8 octobre 2024. https://apnews.com.

AUBY, Jean-Bernard, La globalisation, le droit et l'État. Paris : Montchrestien, 2003, p. 14., cité dans COLLE SECK, Ami,. « Intégration et Souveraineté étatique, approche comparatives entre l'Europe et l'Afrique à travers l'UE, l'UEMOA et l'OHADA », thèse de doctorat en droit, Normandie Université, 2018, p.3.

Australian Government, « 2023–2030 Australian Cyber Security Strategy », Commonwealth of Australia, 2023, p. 30. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

ÁVILA Eça de Matos, B., DANE, G. Z., VAN TILBURG, T., VERSTAPEN, J., et de VRIES, B., « State-of-the-Art of the Urban Digital Twin Ecosystem in the Netherlands », In M. Jalonen (Ed.), Smart Cities in Smart Regions 2022 Conference Proceedings, LAB University of Applied Sciences, pp. 37-53, 2022.

AWS, « Pilier Efficacité des performances », AWS Framework Well-Architected, p. 65, 2024. https://docs.aws.amazon.com/fr_fr/wellarchitected/latest/performance-efficiency-pillar/wellarchitected-performance-efficiency-pillar.pdf.

B. R. Barricelli, E. Casiraghi, et D. Fogli, « A survey on digital twin : definitions, characteristics, applications, and design implications, », 2019.

BAEZNER Marie, et ROBIN Patrice, « Cyber sovereignty and data sovereignty », ETH Zurich, 2018. https://www.research-collection.ethz.ch/handle/20.500.11850/314613

BARRACO Laurent, « La bulle opérationnelle aéroterrestre », La Jaune et la Rouge, n° 615, mai 2006.

BARRETT Lindsey, « Confiding in con men : US privacy law, the GDPR, and information fiduciaries », Seattle University Law Review, 42, 2018. https://digitalcommons.law.seattleu.edu/sulr/vol42/iss3/5/

BARTHE Emmanuel, « Les normes, l'AFNOR et leur financement — Ou pourquoi les normes ne sont pas près de devenir gratuites », Précisément [blog], novembre 2021. https://www.precisement.org/blog/Les-normes-l-Afnor-et-leur-financement-Ou-pourquoi-les-normes-ne-sont-pas-pres.html.

BARTHE Emmanuel, « Vers une privatisation des normes ? », décembre 2009.

Base Camp Connect, « Au-delà des cryptomonnaies : Comment la blockchain protège les réseaux gouvernementaux et militaires », 13 novembre 2024. https://basecampconnect.com/fr/blockchain-reseaux-militaires/

BAUD Michel, « Cyberguerre : en quête d'une stratégie », Ifri, focus stratégique n° 44, mai 2013, p. 34.

BEEK (van de) S. et LEFERINK F., « Vulnerability of Remote Keyless-Entry Systems Against Pulsed Electromagnetic Interference and Possible Improvements », IEEE Transactions on Electromagnetic Compatibility, 1er août 2016, pp. 1259–1265.

BECKLEY M., « China's century? Why America's edge will endure », in International Security, Vol.36, N°3, pp.41-78, Hiver 2011/12.

BECKWITH, Richard, SHERRY John, et PRENDERGAST David, « Data flow in the Smart City : Open data versus the commons », In M. de Lange & M. de Waal (Eds.), in The Hackable City, Springer, 2019, pp. 205–221. https://link.springer.com/chapter/10.1007/978-981-13-2694-3_11.

BELLANGER Pierre, La souveraineté numérique, Paris, Stock, 2014, p. 12.

BELTRAN Jacques, « Les jumeaux numériques pour moderniser les villes de demain », BatInfo / Dassault Systèmes, 4 février 2021.

BENEZECH Danièle, « La norme : une convention structurant les interrelations technologiques et industrielles », Revue d'économie industrielle, vol. 75, Normalisation et organisation de l'industrie., 1er trimestre 1996, P. 34.

BERTINO Elisa, Thuraisingham Bhavani, Gertz Michael, et Damiani Maria Luisa, « Security and privacy for geospatial data », Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS, novembre 2008.

BODIN Jean, Les Six Livres de la République, Paris, 1576, Livre I, chapitre VIII.

BOMONT Clotilde, « Le cloud défense : défi opérationnel, impératif stratégique et enjeu de souveraineté », Policy Commons Focus stratégique, n° 107, IFRI, novembre 2021, 64 p.

BORODYNA Olena, « Russia's recent ITU election loss is a major setback for China's internet governance ambitions », ODI, 5 octobre 2022.

BOOZ Allen Hamilton, « Geospatial Interoperability Return on Investment Study », National Aeronautics and Space Administration (NASA), Geospatial Interoperability Office, Avril 2005.

BORGES Rose-Marie et Munier Manuel, « Qualification juridique des données numériques », Convergences du Droit et du Numérique 2017, septembre 2017, Bordeaux, France.

Borrell Josep, discours d'ouverture du Collège d'Europe, Bruges, 13 octobre 2022. Disponible sur : https://www.eeas.europa.eu/eeas/building-more-muscular-european-foreign-policy-speech-high-representative-borrell_en

BOULANGER, Philippe, « La géographie reine des batailles », Perrin, 2020.

BOWKER Geoffrey C., STAR Susan Leigh, Sorting Things Out : Classification and Its Consequences, Cambridge (MA), MIT Press, 1999.

BRADFORD Anu, The Brussels Effect : How the European Union Rules the World, Oxford, Oxford University Press, 2020, p.2.

BRADFORD Anu, « The Brussels Effect : How the European Union Rules the World », Oxford University Press, 2020, pp. 833-838.

BRADSHAW & Ryan, ODI, 2022

BRUNSSON Nils, JACOBSSON Bengt (dir.), A World of Standards, Oxford, Oxford University Press, 2000, p. 1.

BSI, « Technical guideline on cryptographic mechanisms : Recommendations and key lengths », 2023. . Consulté le 6 janvier 2024. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile.

BURRIN Philippe, « La France à l'heure allemande (1940-1944) », Paris, Seuil, p. 321, 1995.

BUTERIN Vitalik, « Ethereum White Paper : A Next-Generation Smart Contract Platform », GitHub, 2014. Disponible sur : https://github.com/ethereum/wiki/wiki/White-Paper

BUTHE Tim, MATTLI Walter, The New Global Rulers : The Privatization of Regulation in the World Economy, Princeton, Princeton University Press, 2011, p. 3.

CARGILL Carl F., « Information Technology Standardization : Theory, Process and Organizations », Bedford : Massachusetts, Digital Equipment Corporation, 1er janvier 1989.

CATTARUZZA Amaël, « Géopolitique des données numériques : Pouvoir et conflits à l'heure du Big Data », Paris, Le Cavalier Bleu, 2019, p. 15.

CATTARUZZA Amaël, Music Maylis, « La guerre en Ukraine, premier conflit de haute intensité à l'ère numérique », Hérodote, n° 186-187, 2022, pp. 7-24.

CDEF et DREUX, « Géographie et combat en zone urbaine », in Cahier de la recherche doctrinale, Centre de doctrine d'emploi des forces, janvier 2005.

CEBROWSKI Arthur K., et GARSTKA John H., « Network-Centric Warfare - Its Origin and Future », Proceedings, Vol. 124, janvier 1998.

CEBROWSKI Arthur K., « Network-Centric Warfare : Its Origin and Future », US Naval Institute Proceedings, janvier 1998.

Central Committee of the Communist Party of China and the State Council, « Outline for the development of national standardization », Xinhua, 10 octobre 2021.

CEPICKY Jachym, Switch from Shapefile, 8 octobre 2017. http://switchfromshapefile.org.

Cerema, « Standard Friches, Structure de données ouvertes pour inventorier et caractériser les friches », (version 2022 – rev. V2023-12), 2023, p. 6.

CHANDER Anupam, et Lê Uyen P., « Data nationalism », Emory Law Journal, n° 64, 2015, pp. 677–740. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/.

CHARLIE Parker, « Uber-style technology helped Ukraine to destroy Russian battalion », The Times, mai 2022.

CHEN Jinliu, WENQUAN Gan, NING Liu et al., « Community Quality Evaluation for Socially Sustainable Regeneration : A Study Using Multi-Sourced Geospatial Data and AI-Based Image Semantic Segmentation », International Journal of Geo-Information, Disponible ici : 13(5), p. 167, 2024. . Consulté le 13 avril 2025.https://www.mdpi.com/2220-9964/13/5/167.

CHEN Maggie Xiaoyang, et MATTOO Aaditya, « Regionalism in Standards : Good or Bad for Trade? », World Bank, octobre 2004.

China Standards 2035 et National Standardization Development Outline (CSET Georgetown, 2021.

CHIRIO Maud, « Le pouvoir en un mot : les militaires brésiliens et la « révolution » du 31 mars 1964 », in Nuevo Mundo, Mundos Nuevos, n°7, 2007.

CHO Sungbaek et al., « Cybersecurity Considerations in Autonomous Ships », NATO Cooperative Cyber Defense Center of Excellence (CCDCOE), Tallinn, 2022.

CLAVAL Paul, « Les espaces de la politique, », Paris, Armand Colin, mai 2010, pp. 15 – 16.

CNIL, « LA SÉCURITÉ DES DONNÉES PERSONNELLES », Le Guide de la CNIL, Ed. 2018, 2018, p. 20. https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_guide_securite_personnelle.pdf

Communiqué de presse ANSSI, « Blue OLEx 2020 : les États membres de l'Union européenne lancent le cyber Crisis Liaison Organisation Network (cyclone) », Paris, 29 septembre 2020.

Congrès national populaire, « Loi de normalisation de la République populaire de Chine », Chine, 2017. Traduction anglaise disponible à l'adresse suivante : https://www.cfstc.org/en/2932583/2968817/index.html

Congrès national populaire, « Loi sur les investissements étrangers de la République populaire de Chine », Chine, 2019. Traduction anglaise disponible à l'adresse suivante : https://en.ndrc.gov.cn/policies/202105/t20210527_1281403.html.

Conseil de l'Union européenne, « Conclusions du Conseil sur la diplomatie numérique de l'UE », doc. 10526/23, Bruxelles, 26 juin 2023.

Conseil de l'Europe, « Étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données et éventuelles implications réglementaires », DGI et MSI-NET, 2017, p. 41.

COOPER A et al., Request for Comment (RFC) 6973 : « Privacy Considerations for Internet Protocols », Internet Architecture Board, 2013. https://datatracker.ietf.org/doc/html/rfc6973.

Cour permanente d'Arbitrage, « Sentence arbitrale rendue le 4 avril 1928, par M. Max Huber, entre les États-Unis et les Pays-Bas, dans le litige relatif à la souveraineté sur l'île de Palmas (ou Miangas) », traduit par M. Ch. Rousseau, in Revue générale de Droit international public, p. 156, 1935.

COUTURE Stéphane, Toupin Sophie, « What does the notion of 'sovereignty' mean when referring to the digital? », New Media & Society, vol. 21, n° 10, 2019, pp. 2305-2322.

CRANE Rhonda J., « The Politics of International Standard Setting : France and the Color TV War. », Norwood, 1979.

CROOK Anthony, « Allied Command Operation Geospatial Handbook. », OTAN, Naples, 30 juillet 2009.

CURBERA Francisco, Hallam-Baker Phillip, VeriSign Maryann Hondo, Nadalin Anthony, Nagaratnam Nataraj, et Sharp Chris, « Web services policy framework (ws-policy) », Policy, 2006.

CUTLER A. Claire, Haufler Virginia, Porter Tony (dir.), Private Authority and International Affairs, Albany, Suny Press, 1999.

Cybersecurity & Infrastructure Security Agency, « Post-Quantum Cryptography Initiative », 2021. https://www.cisa.gov/quantum

DABROWSKI Andrzej, « The Clean Network Initiative as an Element of the U.S.-China Competition »,PISM Polski Instytut Spraw Międzynarodowych, 2021. https://www.ceeol.com/search/gray-literature-detail?id=1164684

DANA Heide, Kewes Tanja et Müller Anja, « Anti-Spionage-Gesetz beunruhigt deutsche Unternehmen », Handelsblatt, 20 juin 2023.

DANIEL R. Russel et Blake H. Berger, « Stacking the Deck : China's Influence in International Technology Standards Setting », The Asia Society Policy Institute, 2021.

DARNIS Jean-Pierre, « Sécurité et défense spatiale de l'Union européenne », in L'Année de la Défense nationale - Ruptures stratégiques. Quels enjeux pour la France et pour l'Europe ?, la documentation française, 2024. https://shs.cairn.info/article/LDF_DURIEU_2024_01_0115

DASKAL, J., « Law enforcement access to data across borders : The evolving security and rights issues », Journal of National Security Law and Policy, n° 8, 2016, pp. 473–502. https://jnslp.com/wp-content/uploads/2017/10/Law-Enforcement-Access-to-Data-Across-Borders_2.pdf.

DAVID P., « Some new standards for the economics of standardization in the information age », in Dasgupta P. et Stoneman P. , Economic Policy and Technological Performance, Cambridge University Press, Cambridge, 1987, pp. 206 – 239.

DAVID Paul A., « Clio and the Economics of QWERTY », The American Economic Review, vol. 75, n° 2, 1985, pp. 332-337.

DAVID Paul A., « Some New Standards for the Economics of Standardization in the Information Age », in DASGUPTA Partha, Stoneman Paul (dir.), Economic Policy and Technological Performance, Cambridge, Cambridge University Press, 1987, pp. 206-239.

DE Vries, H. et al., « SME access to European standardization : Enabling small and medium-sized enterprises to achieve greater benefit from standards and from involvement in standardization », ResearchGate, août 2009.

Délégués commerciaux Canada, « La loi sur la cybersécurité – Chine . Liste des agences impliquées dans la mise en œuvre », 2024.

DELPHI Group, « The Value of Standards : A Delphi Study », Boston (Massachusetts), juin 2003.

DEMIANOV G.V., Kaftan V.I., Makarenko N.L., Zabnev V.I., Zoubinski V.I., « New Russian Reference Frame : Status and Development », in National Reports, 2000, pp. 293 – 300. .

https://d1wqtxts1xzle7.cloudfront.net/47879547/New_Russian_Reference_Frame_Status_and_D20160808-30010-y9xmld-libre.pdf Consulté le 23 janvier 2025.

DENARDIS Laura, « Protocol Politics : The Globalization of Internet Governance », Cambridge (MA), MIT Press, 2009, p. 6.

Department of Defense, « Executive Summary : DoD Data Strategy : Unleashing Data to Advance the National Defense Strategy », Office of Prepublication and Security Review, 30 septembre 2020, p. 7.

DESBOIS Henri, « La carte et le territoire à l'ère numérique », Socio, n° 4, 2015.

Developpez.com, « La nouvelle loi chinoise sur la cybersécurité entre en vigueur le 1er juin », 2017.

DEVILLIERS Olivier, « L'interopérabilité, enjeu central du jumeau numérique national », 2 juin 2024. https://www.banquedesterritoires.fr.

DIARRAH Séga, « La Blockchain dans la prévention et la gestion des conflits sociaux en Afrique : cas du foncier au Mali », Working Paper, 2022.

DIETER Ernst, « Indigenous Innovation and Globalization : The Challenge for China's Standardization Strategy », UC Institute on Global Conflict and Cooperation and the East-West Center, juin 2011.

Direction de l'information légale et administrative , « Livre blanc Défense et Sécurité nationale », p. 70, 2013.

Direction de l'information légale et administrative, « Livre Blanc Défense et Sécurité nationale 2013 », Paris, 2013, p. 94.

Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État, « Référentiel Général d'Interopérabilité : Standardiser, s'aligner et se focaliser pour échanger efficacement », version 2.0, décembre 2015. https://www.numerique.gouv.fr/publications/interoperabilite/.

CHOI Dong-Geun et Erik Puskar, « A Review of U.S.A. Participation in ISO and IEC, Standards Coordination Office Laboratory Programs », National Institute of Standards and Technology, U.S. Department of Commerce (NISTIR 8007), juin 2014.

CHOI Dong-Geun et Psukar Erik, « A Review of U.S.A. Participation in ISO and IEC, Standards Coordination Office Laboratory Programs », National Institute of Standards and Technology (NIST), U.S. Department of Commerce (NISTIR 8007), juin 2014.

DOSHI Rush, de La Bruyère Emily, Picarsic Nathan et Ferguson John, « China as a « Cyber Great Power » : Beijing's two voices in communications », Foreign Policy, Security, strategy and order, BOOKINGS, avril 2021, p.10.

DOUGLAS M. David, Lacey Justine & Howard David, « Ethical risk for AI », AI Ethics, 2024. https://link.springer.com/article/10.1007/s43681-024-00549-9

DOUZET Frédérick, Desforges Alix, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », Hérodote, n° 177-178, 2020, pp. 3-15.

DOUZET Frédérick, « La géopolitique pour comprendre le cyberespace », Hérodote, n° 152-153, 2014, p. 4.

DREZNER Daniel W., « All Politics Is Global : Explaining International Regulatory Regimes, Princeton », Princeton University Press, 2007.

DUDOUET et coll., « Politiques internationales de normalisation » quelques jalons pour la recherche empirique », revue française de science politique, vol. 56, 2006, p. 367 – 392.

DUFFAUX Karine, « La Démarche productive : une approche en termes d'héritage, la perspective allemande. », 1995.

EABRASU Marian, « Les états de la définition wébérienne de l'État », Raisons politiques, n° 45, p.187, 2012.

EGIS Conseil, « Miroir, miroir… : le jumeau numérique du territoire », La Banque des Territoires, p. 9, juillet 2021.

ELIOT Cohen, « NATO Standardization : The Perils of Common Sense. », in Foreign Policy, no. 31, pp. 72 – 90, 1978.

ELWOOD Sarah, « Grassroots groups as stakeholders in spatial data infrastructures : Challenges and opportunities for local data development and sharing », International Journal of Geographical Information Science, n° 22, 2008, pp. 71–90 https://www.tandfonline.com/doi/abs/10.1080/13658810701348971

ENDRACA Alexander, King Bryan, Nodalo George, Sta Maricone, Sabas Maria et Isaac, « Web Application Firewall (WAF) », in International Journal of e-Education, e-Business, e-Management and e-Learning, Vol. 3, n° 6, décembre 2013. https://www.ijeeee.org/index.php?m=content&c=index&a=show&catid=41&id=595

ENISA, « Post-Quantum Cryptography : Current state and quantum mitigation », 3 mai 2021. . Consulté le 22 octobre 2024.

ETO Manabu, « Historical Development of Industrial Standardization in Japan as the Background of the Current Standards and Conformity Assessment Policy » (工業標準化政策の変遷と基準認証政策), The Journal of Science Policy and Research Management, n°22, 2007.

EUNICE P., « Human Geography Depicts Cultural Terrain », Pathfinder, Vol. 8, No. 5, 2010.

EUROCONSULT, « Space Economy Report », 2023 cité dans « Étude économique de l'écosystème géonumérique en France », Afigéo, p. 47, septembre 2024. https://www.afigeo.asso.fr/wp-content/uploads/2024/09/16/etude-economique-ecosysteme-geonumerique-afigeo.pdf

European Parliamentary Research Service, « Key enabling technologies for Europe's technological sovereignty », Scientific Foresight Unit (STOA), PE 697.184, décembre 2021, pp. 113, p. 16.

EZRA Chipatiso, « Application of GIS and Artificial Intelligence in Military Operations: Prospects and Challenges », Space and Defense, 2022.

Fédération de Russie et République populaire de Chine, « Joint Statement of the Russian Federation and The People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Developement », Beijing, 4 février 2022, partie III.

FARREL Joseph, SALONER Garth, « Coordination Through Committees and Markets », The RAND Journal of Economics, vol. 19, n° 2, 1988, pp. 235-252.

FAVEREAU Olivier, « Marchés internes, marchés externes », Revue économique, vol. 40, n° 2, 1989, pp. 273-328.

FÉDÉRAL Bureau of investigation, « China's Standards 2035 Plan Seeks to Dominate Standards for Emerging, Disruptive Technologies, and ICT Global Marketplace », Liaison Information Report (LIR), LIR 210303004, 3 mars 2021.

FILIPPO Gualtiero Blancato, "Regulate to Dominate : The Geopolitics of Standard-Setting in Digital Technologies and its Strategic Implications for the EU", UNU-CRIS Institute on Comparative Regional Integration Studies, Policy Brief n° 8, 2019.

FIVE Eyes intelligence Oversight and Review Council, « Charter of the Five Eyes Intelligence Oversight and Review Council », 2 octobre 2017.

FLORIDI Luciano, « The Fight for Digital Sovereignty : What It Is, and Why It Matters, Especially for the EU », Philosophy & Technology, vol. 33, 2020, pp. 369-378.

FLORINI, A., et Dehqanzada, Y., « Commercial satellite imagery comes of age. Issues in Science and Technology », n° 16, 1999, pp. 45–52. https://issues.org/florini/.

FOLASHADÉ Soulé, « Digital Sovereignty in Africa: Moving beyond Local Data Ownership », Centre for International Governance Innovation (CIGI), 2022.

Fortune Business Insight, « Geospatial Imagery Analytics Market Size, Share & COVID-19 Impact Analysis, By Imaging Type (Video and Image), By Collection Medium (Geographic Information System (GIS), Satellite Imagery, and Others), By Application (Weather Conditions Monitoring, Disaster Management, Urban Planning/Development, Natural Resource Exploration, and Others), By End-user (Defense & Security, Healthcare, Retail & Logistics, Government, Banking, Financial Services & Insurance (BFSI), Mining/Manufacturing, Agriculture, and Others), and Regional Forecast, 2023-2030 », 2024. https://www.fortunebusinessinsights.com/geospatial-imagery-analytics-market-108685

FRANCISCO Curbera, Phillip Hallam-Baker, VeriSign Maryann Hondo, Anthony Nadalin, Nataraj Nagaratnam, et Chris Sharp, « Web services policy framework (ws-policy) ». Policy, 2006.

FROCHOT Didier, « Le droit des systèmes d'information géographique », les Infostratèges, 29 septembre 2011.

FROCHOT Didier, « Les systèmes d'information géographique et le droit », Archimag, n° 326, juin 2019, pp. 40-41.

GALRHAN, « Electronic War in IAF Strike in Syria », in Information Dissemination (blog), 16 octobre 2024. https://www.informationdissemination.net/2007/10/electronic-war-in-iaf-strike-in-syria.html

GALULA David, « Contre-insurrection théorie et pratique », Paris, Economica, 2008.

GARANCE Mathias, « Le marché unique des données : quels sont les apports du DGA et du Data Act ? », S&D Magazine, n° 58, septembre 2023.

GAUTAMI Tripathi, Ahad Mohd Abdul et Casalino Gabriella, « A comprehensive review of blockchain technology: Underlying principles and historical background with future landmark pitfalls », Journal of Information Security and Applications, 2022.

MAI Gengchen, JANOWICZ Krzysztof, ZHU Rui, CAI Ling, et Ni Lao « Geographic Question Answering : Challenges, Uniqueness, Classification, and Future Directions », 24th AGILE Conference on Geographic Information Science, 2021. https://agile-giss.copernicus.org/articles/2/8/2021/agile-giss-2-8-2021.pdf

GEOSCIENCE Australia. « Asia-Pacific Reference Frame (APREF) « Geospatial Intelligence Standards Working Group », 28 septembre 2017, « Geospatial Intelligence standard : Part 2 : Overview of GEOINT Standards », On-line training modules sponsored by the Geospatial Intelligence Standards Working Group (GWG), 30 janvier 2007.

Geospatial World (GW Consulting), « Advancing & Augmenting USD 1.4 Trillion Geospatial Market by 2030 — GeoBuiz Report 2022 », Geospatial Media and Communications, 2023. https://geospatialworld.net/gw-market-insights/advancing-augmenting-usd-1-4-trillion-geospatial-market-by-2030/.

Geospatial World, « GeoBuiz Global Geospatial Industry Outlook 2022 », 2022. Disponible ici : https://geospatialworld.net/consulting/reports/geobuiz/2022/index.html#download-ebook

GERSCHENKRON Alexander, « Economic Backwardness in Historical Perspective », Cambridge : Massachusetts, Harvard University Press, 1962.

GIBSON Christopher S., « Globalization and the Technology Standards Game : Balancing Concerns of Protectionism and Intellectual Property in International Standards », Boston, Massachusetts, Suffolk University Law School, Legal Studies Research Paper Series (Research Paper 07-39), 31 octobre 2007.

GILLIES Sean, « GeoJSON-LD », 20 décembre 2021. https://geojson.org/geojson-ld/. Consulté le 12 mars 2025.

Global Defence Technology, « How radars, reconnaissance and software are shaping the artillery war in Ukraine », juin 2022.

GOODCHILD Michael F., « Citizens as sensors : the world of volunteered geography », GeoJournal, vol. 69, n° 4, 2007, pp. 211-221.

GOURINCHAS Pierre-Olivier, « Un casse-tête géoéconomique », Finances & Développement, FMI, juin 2022, pp. 4–7.

GRAVIER Jean-François, Paris et le désert français, Le Portulan, 1947.

GRAZ Jean-Christophe, La gouvernance de la mondialisation, Paris, La Découverte, 2013, p. 78.

GRIEVES M., « Digital twin : manufacturing excellence through virtual factory replication : a whitepaper », 2014.

GRIEVES M. et VICKERS J., « Digital twin : Mitigating unpredictable, undesirable emergent behavior in complex systems, » in Transdisciplinary perspectives on complex systems, pp. 85–113, Springer, 2017.

GROS Philippe, « Le « cloud tactique« , un élément essentiel du système de combat aérien du futur », Fondation pour la Recherche scientifique, note n° 8/19, 19 juin 2019.

Groupe d'Études Géopolitiques, « L'Europe comme puissance normative internationale : état des lieux et perspectives », 2024.

GROVER Lov, « A fast quantum mechanical algorithm for database search », dans Proceedings, 28th Annual ACM Symposium on the Theory of Computing, 1996, p. 212. https://arxiv.org/abs/quant-ph/9605043

GUIDE ISO/CEI 59 : 1994, « Code de bonne pratique pour la normalisation », paragraphe 1.2.

GUNTHER Mackenzie, « Digital Sovereignty in ASEAN », PS-engage, 2024. . Consulté le 2 janvier 2025. https://ps-engage.com/digital-sovereignty-in-asea/

HABER Samuel, « The Quest for Authority and Honor in the American Professions, 1750-1900 ». Chicago, University of Chicago Press, 1991.

HALL Peter A. et Soskice David W., « Varieties of capitalism : the institutional foundations of comparative advantage », Oxford, Oxford University Press, 2001.

HANASHIMA Makoto, « Consideration for information security issues in geospatial information services of local governments ». IASSIST Quarterly, n°29, 2006.

HANDWIKI, « Software : GIS Arta », 7 mars 2023.

HARVEY, F., et Tulloch, D., « Local-government data sharing : Evaluating the foundations of spatial data infrastructures », International Journal of Geographical Information Science, n° 20, 2006, pp. 743–768. https://www.researchgate.net/publication/220649844_Local-Government_Data_Sharing_Evaluating_the_Foundations_of_Spatial_Data_Infrastructures

HAWKINS Richard, MANSELL Robin, SKEA Jim (dir.), Standards, Innovation and Competitiveness : The Politics and Economics of Standards in Natural and Technical Environments, Cheltenham, Edward Elgar, 1995.

HENK J. de Vries et Tineke M. Egyedi, « Standardization Education : Developments and Progress », New Applications in IT Standards : Developments and Progress, janvier 2010.

BERTHAUT Henri-Marie-Auguste, Les ingénieurs géographes français (1624-1831), Paris, Imprimerie du Service géographique, 1902.

HESSER Wilfried, « Memorandum on Standardization in higher Education in Europe », Hambourg, Allemagne, 2014.

HEXAGON, « END-TO-END GEOSPATIAL SOLUTIONS FOR MILITARY LAND C2 OPERATIONS », White Paper, 15 avril 2019.

High-level Forum on European Standardisation, « Education & Skills on Standards », 30 novembre 2023, p. 3.

https://pad.undp.org.mx/files/g/820dcf0c1242364677545293.44594fd/banco/archivo/107/0/benefits-adoption-barriers-and-myths-of-open-data-and-open-government.pdf

Hihg Level Forum on European Standardisation, « Alignment between Europen and International Standards », rapport final du chantier n°4 (pilote : Orgalim), Ares (2025)288593, 15 janvier 2025

HU, G. et al., . « Report on the Asia Pacific Reference Frame (APREF) Project« , UN-GGIM-AP., 2019

HUAWEI et al., New IP, « Shaping Future Network : Propose to Initiate the Discussion of Strategy Transformation for ITU-T. Proposal to ITU-T TSAG », 2019. http://prod-upp-image-read.ft.com/ec34d7aa-70e6-11ea-95fe-fcd274e920ca.

Human Rights Council [HRC], Resolution A/HRC/RES/47/23 : « New and Emerging Digital Technologies and Human Rights », 2021. https://undocs.org/Home/Mobile

HUMMEL Patrick, Braun Matthias, Tretter Max, et Dabrock Peter, « Data sovereignty : A review ». Big Data & Society, 8, 2021. https://journals.sagepub.com/doi/10.1177/2053951720982012

HUMPHREYS Todd E., « Statement on the Vulnerability of Civil GPS to Spoofing Attacks », U.S. House of Representatives Committee on Homeland Security, 2022.

HUNTLEY Robert, « Quantum-Enabled PNT Protects Against GNSS Outages », EE Times Europe, 18 novembre 2024. https://www.eetimes.eu.

HURA M., et coll., « Interoperability : a continuing challenge in coalition operations », Santa Monica, RAND, 2000.

HYUNJUN Kim, Wonwoong Kim, Yeajun Kang, Hyunji Kim et Hwajeong Seo, « Post-Quantum Delegated Proof of Luck for Blockchain Consensus Algorithm », Appl. Sci. 14(18), 8394, 18 septembre 2024. https://doi.org/10.3390/app14188394. Consulté le 25 octobre 2024.

IBM, « Server audit log settings », IBM Security Directory Server, 21 février 2024. https://www.ibm.com/docs/en/sdse/6.4.

IDB (Banque interaméricaine de développement), «Distributed Ledger Technology (Blockchain): The Future of Land Titling and Registry », 19 juillet 2019. https://www.iadb.org.

IGN, « Les territoires, coproducteurs du référentiel LiDAR HD France entière », communiqué de presse, Saint-Mandé, 23 novembre 2023.

IGN, « Point d’information sur le projet de couverture nationale en données Lidar HD », Réunion interrégionale du 15 décembre 2022, p. 1.

IGO, « Jumeau numérique du Département de l'Aude – GEODATADAYS 2022 : Un autre usage des données PCRS pour répondre aux enjeux régionnaux et ruraux », 2022. https://www.igo.fr/laval-virtual-et-geodatadays-2022/

IMBERT Vincent, « La bulle opérationnelle aéroterrestre (BOA) : un choix nécessaire », RDN, n°643, juin 2022, pp. 97 – 106.

INCIBE, « Cybersecurity challenges of digital twins: threats and security measures », 5 septembre 2024. https://www.incibe.es.

INPI, « L'informatique quantique dans les brevets en 2024 », novembre 2024. https://www.inpi.fr.

INRIA, « Quels sont les principaux acteurs de l'informatique quantique ? », 16 décembre 2020. https://www.inria.fr/fr/acteurs-informatique-quantique.

INSPIRE work program 2021-2024, Action 2.1 Need-driven data prioritisation.

Institut Ign, « LiDAR HD : vers une nouvelle cartographie 3D du territoire », 2024. https://www.ign.fr/institut/lidar-hd-vers-une-nouvelle-cartographie-3d-du-territoire

ISAAC Henri, « Quelle souveraineté numérique européenne ? », in Revue française de gestion, n° 305, 22 août 2022, pp. 63-77.

ISO, « Guide ISO/IEC », partie 2, 2004, p. 4.

ISO/IEC, « Technologies de l'information — Interopérabilité avec les technologies d'assistance, Partie 2 : Interface de programmation d'applications (API) d'accessibilité Windows », TR 13066-2 : 2016, édition 2, février 2016, p. 5.

JAFFEE, S, et Henson, S., « Standards and Agro-Food Exports from Developing Countries : Rebalancing the Debate », World Bank, 2004.

JAMES A. Lewis, « A Strategic Outlook for Cyberspace Operations », in Cyberspace Strategic Outlook 2030 Horizon Scanning and Analysis, NATO CCDCOE Publications, pp. 10- 15, 2022.

JANSSEN Marijn, Charalabidis Yannis, et Zuiderwijk Anneke, « Benefits, adoption barriers and myths of open data and open government », Information Systems Management, n°29, 2012, pp. 258–268.

JARASSÉ Jim, « Les insurgés irakiens piratent les drones américains », Le Figaro, 17 décembre 2009. https://www.lefigaro.fr.

JETT Jennifer, « China's new map outrages its neighbors », NBC News, 1er septembre 2023.

JEUNEMAITRE Julie, « Dans l'Oise, les cyberattaques se multiplient dans les collectivités locales », La Voix du Nord, 2022.

JOHN Agnew, « The Territorial Trap : The Geographical Assumptions of International Relations Theory », in Review of International Political Economy, Vol 1 (1), Spring, 1994, pp. 53-80.

JOHN Seaman, « China and the New Geopolitics of Technical Standardization », Ifri, janvier 2020.

JOHNSON Peter A., « Models of direct editing of government spatial data : Challenges and constraints to the acceptance of contributed data », Cartography and Geographic Information Science, 44, 2017, pp. 128–138. https://www.tandfonline.com/doi/full/10.1080/15230406.2016.1176536

JONES Adrian, « Illusions of Sovereignty : Business and Organization of Committees of Vichy France », in Social History, n° 11, 1er janvier 1986.

JONES Andrew, « China's SAR satellite surge continues with new constellation plan », Space News, 7 décembre 2021. https://spacenews.com.

JOSSE Fanny et Riss Sylvain, « Le jumeau numérique environnemental » à l'échelle du territoire, les données au cœur des cas d'usage », EDP Science, 2024. https://www.shs-conferences.org/articles/shsconf/pdf/2024/18/shsconf_edubim2024_03003.pdf

JOUTALE Fabien, « L'intelligence artificielle de Safran facilite la prise de décisions sur le terrain », Ouest-France, 2023.

JUNQUERA-SÁNCHEZ Javier, HERNANDO-RAMIRO Carlos, GAMALLO-PALOMARES Oscar, GOMEZ-SANCHEZ José-Antonio, « Assessment of cryptographie approches for a quantum-résistant Galileo OSNMA », NAVIGATION : Journal of the Institut of Navigation, Vol. 71(2), 2024. https://navi.ion.org/content/71/2/navi.648

KAIBIN Bao, HRISTO Valev, WAGNER Manuela, et HARTMUT Schmeck, « A threat analysis of the vehicle-to-grid charging protocol iso 15118 », Computer Science-Research and Development, 33, 2018, pp. 3 – 12.

KAIROUANI Ali, « Le pouvoir normatif des entreprises multinationales en droit international », Revue internationale de droit économique, t. XXXIV, 2020/3, pp. 253 – 295.

KAMENSKY Jack, « Standards Setting in China : Challenges and Best Practices »,The US-China Business Council, janvier 2020.

KAORU Kenyoshi et Hao Qin, « Framework of quantum key distribution (QKD) protocols in QKD network », ITU, 2024. . Consulté le 7 mars 2025. https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18760

KEDAR john, « Ethical Standards and Transparency Can Protect Location Data », Geospatial world, 2024. https://geospatialworld.net/prime/special-features/ethical-standards-and-transparency-can-protect-location-data/

KELLER Reto, « EU Harmonized Standards - What does that mean? », Academy of EMC, 11 juin 2024. https://www.academyofemc.com.

KELVIN Lawrence, Chris Kaler, Anthony Nadalin, R Monzillo, et P Hallam-Baker. « Web services security : Soap message security 1.1 (ws-security 2004) ». OASIS, OASIS Standard, Février 2006.

KELVIN Lawrence, Kaler Chris, Nadalin Anthony, Monzillo R, et Hallam-Baker P, « Web services security : Soap message security 1.1 (ws-security 2004) », OASIS, OASIS Standard, Février 2006.

KEMPF Olivier, « Introduction à la cyberstratégie », Paris, Economica, p. 76, 2012.

KEN Alder, The Measure of All Things : The Seven-Year Odyssey and Hidden Error That Transformed the World, New York, Free Press, 2002.

KHRONOS Group, « OGC and Khronos Form a Liaison to Improve Interoperability within the Geospatial and 3D Graphics Communities », 2020. https://www.khronos.org.

KIPP Jacob, Lester Grau, Prinslow Karl et coll., « The Human Terrain System », Military Review, sept.-oct. 2006.

KISA, « Quantum-résistant cryptographie », 2025 https://seed-kisa-or-kr.translate.goog/kisa/ngc/pqc.do?

Köhler Sebastian, Baker Richard, Strohmeier Martin, et Martinovic Ivan, « Brokenwire : Wireless disruption of ccs electric vehicle charging », 2022.

KOSINSKI Matthew et Forrest Amber, « Qu'est-ce que la confidentialité des données ? », IBM, 19 décembre 2023. https://www.ibm.com.

KOUNADI O. et Leitner M., « Why Does Geoprivacy Matter? The Scientific Publication of Confidential Data Presented on Maps », Journal of Empirical Research on Human Research Ethics, vol. 9, n° 4, 2014, p. 34-45.

KPMG, « Le Cloud européen : de grands enjeux pour l’Europe et cinq scénarios avec des impacts majeurs d’ici 2027-2030 », avril 2021, p. 49.

KRASNER Stephen D., Sovereignty : Organized Hypocrisy, Princeton, Princeton University Press, 1999, pp. 3-4.

KRENILA Michal, « Quantum technology for military applications », EPJ Quantum Technology, vol. 8, n° 24, 2021. https://epjquantumt.springeropen.com.

KULK Stefan, et Van Loenen Bastiaan, « Brave new open data world? », International Journal of Spatial Data Infrastructures Research, 7, 2012, p. 196–206.

KUMMITHA Rama Krishna Reddy, « Smart technologies for fighting pandemics : The techno- and human- driven approaches in controlling the virus transmission », Government Information Quarterly, 37, 2020.

KURBALIJA Jovan, « Introduction à la gouvernance de l'Internet », DiploFoundation, 2011, p. 40. https://www.diplomacy.edu/wp-content/uploads/2012/02/IG20book20-20French-1.pdf

KWAN M.-P., Casas I. et Schmitz B. C., « Protection of geoprivacy and accuracy of spatial information : How effective are geographical masks? », Cartographica, vol. 39, n° 2, 2004, p. 15-28.

La DGNUM (Direction générale du numérique) s'est substituée à la Direction générale des systèmes d'information et de communication (DGSIC) en 2018, avec pour mission de piloter la transformation numérique du ministère.

LACOSTE Yves, Dictionnaire de Géopolitique, Flammarion, 1993. Voir également Subra Philippe, Géopolitique de l'Aménagement du Territoire, Armand Colin, 2007.

LACOSTE Yves, La géographie, ça sert d'abord à faire la guerre, Paris, Maspero, 1976 (réédition La Découverte, 2014), p. 9.

LACOSTE Yves, La géographie, ça sert, d'abord, à faire la guerre, Maspero, 1976.

LACOSTE Yves, « La géographie », in Badie Bertrand, Smouts Marie-Claude (dir.), Le retournement du monde. Sociologie de la scène internationale, Paris, Presses de Sciences Po/Dalloz, 1992, p. 33.

LANGLOIS-BERTHELOT Jean et Gaie Christophe, « Cryptographie : comment se protéger à l'ère quantique ? », Polytechnique Insight, 2024. . Consulté le 23 février 2025. https://www.polytechnique-insights.com/tribunes/geopolitique/cryptographie-comment-se-proteger-a-lere-post-quantique

LATHA Reddy et Anoushka Soni, « Is There Space for a Digital Non-Aligned Movement? », in New Conditions and Constellations in Cyber, Cyberstability Paper Series, The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace , 2021. . https://hcss.nl/wp-content/uploads/2021/09/Is-There-Space-for-a-Digital-Non-Aligned-Movement.pdfConsulté le 10 mars 2024.

LAZONICK William et March Edward, « The rise and demise of Lucent Technologies », University of Massachusetts, Dartmouth College, 2010.

Le Genissel Rémi et Vigouroux Gauthier, « Analyzing Cybersecurity Risk within a Geographic Standards Ecosystem », DGIWG Technical Panel Meeting, 8 avril 2024.

Le Monde du Droit, « Loi de Cybersécurité en Chine » , p. 1, 28 septembre 2017.

LEDESMA Josue, « Qu'est-ce que la gestion des accès à privilèges (PAM) ? », Varonis, 6 octobre 2023. https://www.varonis.com/fr.

LEE Kai-Fu, AI Superpowers : China, Silicon Valley, and the New World Order, Boston, Houghton Mifflin Harcourt, 2018, 272 p.

LÉPINARD Philippe et Null Pastorelli Ivan, « Numérisation de l'espace de Bataille : une opportunité pour le développement durable », XVe Conférence AIM, mai 2010. https://hal.science/hal-02133848.

LESSIG Lawrence, Code and Other Laws of Cyberspace, New York, Basic Books, 1999, p. 6 : « Code is law ».

LESSIG Lawrence, « Code and Other Laws of Cybersoace", Basic Books, Newy York, 1999. (PDF) Code and other laws of cyberspace.

LESZCZYNSKI Agnieszka, « Speculative futures : Cities, data, and governance beyond smart urbanism », Environment and Planning A : Economy and Space, n° 48, 2016, pp. 1691–1708 https://www.researchgate.net/publication/303470840_Speculative_futures_Cities_data_and_governance_beyond_smart_urbanism

Lettre du ministre des Armées Sébastien Lecornu, 3 décembre 2024, citée par L'Informé, 24 décembre 2024.

LIU, X., Han, J., ZHONG, Y., HAN, C., HE X., « Implementing WebGIS on hadoop : A case study of improving small file i/o performance on HDFS. », IEEE international conference on cluster computing and workshops, Cluster' 09, pp. 1–8, 2009.

LIVRE blanc sur la défense et la sécurité nationale, 2013.

LIZE Sanderson, « Point Cloud to 3D Terrain Model with Buildings », 2024. https://support.safe.com/hc/en-us/articles/25407508246413-Point-Cloud-to-3D-Terrain-Model-with-Buildings

LONGLEY P A et al., « New Developments in Geographical Information Systems : Principles », Techniques, Management and Applications-2nd edition, 2004, p. 693.

LOQUET Véronique, « Enquête exclusive sur la rémunération des fonctions RSSI », CESIN, 7 octobre 2021 www.cesin.fr/

LORENZO Franceschi-Bicchierai, « Fancy Bear Hack of Ukrainian Artillery Fighters Shows Future of War », Vice, 22 décembre 2016.

LUEBBERT Gregory M., « Liberalism, Fascism, or Social Democracy : Social Classes and the Political Origins of Regimes in Interwar Europe », New York, Oxford University Press, 25 juillet 1991.

LVIV Herald, « A Forensic Examination of GIS Arta », 6 juillet 2025 : « Russian forces have tried repeatedly to compromise GIS Arta through cyberattacks and electronic warfare, but without lasting success—due to both hardened encryption and the agility of Ukraine's IT Army in countering threats ».

MAERTENS Miet et Swinnen Johan F.M., « Trade, Standards, and Poverty : Evidence from Senegal », World Development Vol. 37, No. 1, pp. 161–178, 2009.

Makina Corpus, « IA & cartographie : l'IA pour créer des cartes », 2019. https://makina-corpus.com.

MALMIO Irja, « Ethics as an enabler and a constraint – Narratives on technology development and artificial intelligence in military affairs through the case of Project Maven », in Technology in Society, n° 72, 4 janvier 2023. https://doi.org/10.1016/j.techsoc.2022.102193

MARSEILLE Caa, 7 févr. 2008, n° 05MA01729 – CAA Douai, 15 nov. 2007, n° 06DA00335.

MARZOLF Emile, « La gouvernance de la donnée géographique mute pour s'adapter au numérique », Acteurs Publics, 8 septembre 2020.

MATHEUS Andreas, « Testbed-11 engineering report : Implementing common security across the ogc suite of service standards », Technical report, Open Geospatial Consortium, 2015.

MATHEUS Andreas et HERRMANN J, « Geospatial extensible access control markup langage (geoxacml) », Open Geospatial Consortium Inc. OGC, 2008.

MATHEUS Andreas, « Geospatial eXtensible Access Control Markup Language (GeoXACML) », W3C PLING Meeting, Universität der Bundeswehr München, 2009. https://www.w3.org/Policy/pling/wiki/images/5/59/GeoXACML.pdf

MATTLI Walter, BÜTHE Tim, « Setting International Standards : Technological Rationality or Primacy of Power? », World Politics, vol. 56, n° 1, 2003, pp. 1-42.

MATUTES Carmen et REGIBEAU Pierre, « A Selective Review of the Economics of Standardization : Entry Deterrence, Technological Progress and International Competition », European Journal of Political Economy, vol 12, 1996, pp. 183 – 209.

MAUBON Grégory, « Interopérabilité dans le Metaverse : Jérôme Royan nous parle des standards et de la gouvernance », RA'Pro, 2023.

MAZARD Alexandra, « Lancement du premier satellite à communication quantique QUESS », France Diplomatie, 2 septembre 2016. https://www.diplomatie.gouv.fr.

McCANN David, « E-commerce free trade agreements, digital chapters and the impact on labour : A comparative analysis of treaty texts and their potential practical implications », International Trade Union Confederation, 2019. https://www.ituc-csi.org/IMG/pdf/digital_chapters_and_the_impact_on_labour_en.pdf

MENDES R. et Vilela J. P., « Geoprivacy in Neighbourhoods and Health Research : A Mini-Review of the Challenges and Best Practices in Epidemiological Studies », International Journal of Environmental Research and Public Health, vol. 19, n° 21, 2022.

MENDIBOURE Léo, AYMEN Chalouf Mohammed et KRIEF Francine, « A Scalable Blockchain-based Approach for Authentication and Access Control in Software Defined Vehicular Networks », 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, USA, septembre 2020.

MEYER Zach, « In tech, the death of the Brussels effect is greatly exaggerated », Centre for European Reform (CER), 8 décembre 2023. https://www.cer.eu.

MICHAEL Sutherland, « CSR 2019 : Setting a New Standard : Implications of China's Emerging Standardization Strategy », SAIT China Studies Review, 29 octobre 2019.

MILLS Megane, & de Rijcke, Izaak, « Geomatics and the law\geospatial data : Balancing private ownership and public interest », Geomatica, 70, 2016, pp. 5–149.

MILLS Meghan et de Rijcke Izaak., « Geomatics and the law geospatial data : Balancing private ownership and public interest », Geomatica, n° 70, 2016, pp. 5–149.

Ministère de l'Europe et des Affaires étrangères, « Stratégie internationale de la France pour le numérique », 2020, p. 4. . https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf

MITCHELL Chris, « Out with the old : The cryptographic revolution caused by the threat of quantum computing », Computing conference 2024, p. 15, 2024. https://chrismitchell.net/Talks/240711.pdf

MONOLITH Law Office, « Qu'est-ce que la loi chinoise sur la sécurité des données ? Explication des mesures à prendre pour les entreprises japonaises », Tokyo, 2023.

MOUGAYAR William, The Business Blockchain : Promise, Practice, and Application of the Next Internet Technology, New York, Wiley, 2016, 208 p.

MUELLER Milton, Networks and States : The Global Politics of Internet Governance, Cambridge (MA), MIT Press, 2010, p. 5.

MUSIC Maylis, « La souveraineté numérique : un concept en construction », Études de l'IFRI, Focus stratégique n° 115, mars 2023, pp. 8-12.

MYRIAM Quéméner, « Écosystème numérique : enjeux et défis pour les décideurs », S&D Magazine, n° 58, septembre 2023.

NAGANO Juichi et Fukuda Yasukazu, « The Japanese Standardization Systems : History and Current Status », IEEE Communications standards Magazine, n° 2, septembre 2018.

NAMA Raj Budhathoki., Bertram (Chip) Bruce., et Zorica Nedovic-Budic, « Reconceptualizing the role of the user of spatial data infrastructure », GeoJournal, n°72, 2008, p. 149–160. https://www.researchgate.net/publication/225494825_Reconceptualizing_the_role_of_the_user_of_spatial_data_infrastructure

NARAYANAN Arvind et alii, Bitcoin and Cryptocurrency Technologies, Princeton, Princeton University Press, 2016, 336 p.

National Geospatial-Intelligence Agency, « Geospatial Intelligence standard – Enabling a Commmon Vision », novembre 2006.

National Geospatial-Intelligence Agency, Office of Geospatial-Intelligence Management, National System for Geospatial Intelligence : geospatial intelligence (GEOINT) Basic Doctrine, (Publication 1-0), Septembre 2006.

NATO Allied Command Transformation, « CWIX 2024 : NATO's Largest-Ever Digital Interoperability Exercise Concludes », 21 juin 2024.

NATO CCDCOE, « World's largest cyber defense exercise Locked Shields kicks off in Tallinn », 2023.

NATO, Data Strategy for the Alliance (DaSA), approuvée en février 2025, publiée le 30 avril 2025. https://www.nato.int/cps/en/natohq/official_texts_234937.htm.

NEAHER Giulia, Bray David A., Mueller-Kaler Julian et Schatz Benjamin, « Standardizing the Future : How can the United States Navigate the Geopolitics of International Technology Standards? », Atlantic Council, Geotech Center, 14 octobre 2021, p. 16.

NEDOVIC-BUDIC Zorica, K. Pinto Jeffrey, et Warnecke Lisa, « GIS Database Development and Exchange : Interaction Mechanisms and Motivations », URISA Journal, vol. 16, n° 1, 2004.

New America Foundation, « How Ukraine's « Uber for Artillery » is Leading the Software War Against Russia », 2023.

NICOLE Grajewski, « The Evolution of Russian and Iranian Cooperation in Syria », Center for Strategic and International Studies (CSIS), mars 2023.

NOCETI Julien, « Un Internet en morceaux ? Fragmentation d'Internet et stratégies de la Chine, la Russie, l'Inde et l'Union européenne », Institut Montaigne, 2023.

NOCETTI Julien, « Un Internet en morceaux ? Fragmentation d'Internet et stratégies de la Chine, la Russie, l'Inde et l'Union européenne », Politique étrangère, IFRI, n° 1, 2020, pp. 53–66.

North Atlantic Treaty Organization, « NATO Cyber Defence », Factsheet, avril 2021.

NORTHROP Grumman, « Warship Electronic Chart Display and Information System (WECDIS) », 2013,p.2.
http://www.vscomm.co.th/storage/product/2025/01/9b17932db9116262b6ea836a063418fa.pdf.

NOUCHER Matthieu, « Infrastructures de données géographiques et flux d'information environnementale », NETCOM, vol. 27, n° 1-2, 2013, pp. 89-100.

NOVIKOV Illia, « Russia targets Ukrainian energy infrastructure with massive cruise missile and drone attack », Associated Press, 2024.

OCCAR, « MUSIS Common Interoperable Layer (CIL) Delivered », 17 février 2025. https://www.occar.int.

OCDE, « La dimension économique des normes en matière de technologies de l'information », Paris, OCDE, 1991.

OCDE, « La gouvernance des données dans le secteur public », 2020. https://www.oecd-ilibrary.org/sites/48842dc1-fr/index.html?itemId=/content/component/48842dc1-fr

OECD Business and Financial Outlook, « China's Belt and Road Initiative in the Global Trade, Investment and Finance Landscape », OECD, 2018.

Open Geospatial Consortium, « OGC Web Service Security », OGC 17-007r1, version 1.0, 28 janvier 2019, p.18.

ORIANA Skylar Mastro, « How China is Bending the Rules in the South China Sea », Freeman Spogli Institute, Stanford University, 2021.

OTAN, Stratégie de transformation numérique, 2024.

OTAN, « MC 0296/3 Politiques Geospatiale de l'OTAN », Bruxelles, 2011.

OZTURAN, M., Egeli, B., et F. Bacioglu., « Web-GIS based urban management information system : the case of satellite cities in Istanbul », Management Information Systems, 2004 : GIS and Remote Sensing, n°8, pp.13-21, 2004.

P.-M. Dupuy, Droit international public, Paris, Dalloz, 1992, p. 264.

P3TS - « Plug and Play Positioning and Timing System« , 2024.https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-armes/p3ts-plug-and-play-positioning-and-timing-system

PEAR Channing, « Top 5 Interoperability Standards for Digital Twins », Anvil Labs, 24 février 2025. https://anvil.so.

PELISSERO Nicolas, Merino Laso Pedro et Puentes John. « Impact Assessment of Anomaly Propagation in a Naval Water Distribution Cyber-Physical System »., CSR 2021 : IEEE International Conference on Cyber Security and Resilience, Rhodes, juillet 2021.

PELLETIER Philippe, « La Japonaise. Géopolitique et géographie historique de la surinsularité au Japon », Paris, CNRS éditions, 1997.

PEO IEW&S, « Integrated Sensor Architecture », Integration Directorate, décembre 2023, p.2.

PERNOLLET Jacques, « Le processus d'élaboration des normes techniques aux plans national, communautaire et international », Les Petites Affiches, n° 18, 11 février 1998, pp. 12-14.

PETIT Claire, « Les enjeux de la cybersécurisation du milieu maritime », DEFTECH, n° 3, octobre-décembre 2022.

PETITJEAN Olivier, « Géants du numérique, privatiseurs et marchands d'armes : pourquoi la révolte couve contre la smart city », Observatoire des multinationales, 2019.

PING Wang et Zheng Liang, « Beyond Government Control of China's Standardization System History, Current Status and Reform Suggestions », EWC-NSF workshop Mega Regionalism – New Challenges for Trade and Innovation (MCTI), Honolulu, 27 janvier 2016.

POINTU Frédéric et BRAS Cyril, « Cybersécurité, résilience et souveraineté dans les collectivités territoriales », Revue défense Nationale, n°855, décembre 2022.

POWAR J. et al., « SoK : Managing risks of linkage attacks on data privacy », Proceedings on Privacy Enhancing Technologies, 2023.

PODUVAL Sanjay, « Space Power in the 21st Century », AIR POWER Journal, vol. 4, n° 2, été 2009, p. 80. https://capsindia.org.

POHLE Julia, Thiel Thorsten, « Digital sovereignty », Internet Policy Review, vol. 9, n° 4, 2020, pp. 1-19.

PRATEEK Tripathi, « Post-Quantum Cryptography: The lynchpin of future cybersecurity », Observer Research Foundation, 4 décembre 2023.

PURNELL N., et WOO S., « China's Huawei is determined to lead the way on 5G despite US concerns », Wall Street Journal, 30 mars 2018.

PWC, « Cyber Threats 2022 : A Year in Retrospect », 2023. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html.

QADIR, J., « Internet of everything meets the metaverse : Bridging physical and virtual worlds with blockchain », Comput. Sci. Rev. vol. 54, novembre 2024, 100678. . https://www.sciencedirect.com/science/article/pii/S1574013724000625

Qiushi Magazine, « Xi Jinping : s'efforcer de devenir un centre scientifique et un centre d'innovation majeur dans le monde », Qiushi, n° 15, 2021.

RADA Josef, « Smart Defence : Joint geospatial support in NATO », Geoscape, vol. 13, p. 99, 5 novembre 2019.

RAMOS Gabriela, « Éthique de l'intelligence artificielle », UNESCO, 2024. https://www.unesco.org/fr/artificial-intelligence/recommendation-ethics

RAOUL Gaëtan, « Jumeau numérique : pour RTE, le jeu en vaut la chandelle », LeMagIT, 17 juin 2021. https://www.lemagit.fr.

RAUF Gönenç, « Enjeux industriels des normes dans les technologies de l'information », in Revue d'économie industrielle, n° 39, 1987, pp. 208 – 2019, p. 208. . Consulté le 21 mai 2023. https://www.persee.fr/doc/rei_0154-3229_1987_num_39_1_1251.

RHIND David W., « National and international geospatial data policies », In Geographical information systems : Principles, techniques, management and applications, Volume 2 : Management issues and applications, 1999, p. 767–787. https://www.geos.ed.ac.uk/~gisteac/gis_book_abridged/files/ch56.pdf.

RUHLIG Tim, « Technical Standardization, China, and the Future International Order », Brussels, Heinrich Böll Foundation, 2022, p. 12-15.

RUHLIG Tim, « China, Europe and the New Power Competition over Technical Standards », The Swedish Institute of International Affairs, 2021.

RUHLIG Tim, « The Shape of Things To Come : The Race to Control Technical Standardisation », The Swedish Institute of International Affairs and The European Union Chamber of Commerce in China, 2021.

RICE Nikolai F., « Estonia's digital embassies and the concept of sovereignty », Georgetown Security Studies Review, 2019. https://georgetownsecuritystudiesreview.org/2019/10/10/estonias-digital-embassies-and-the-concept-of-sovereignty/

RIES-MARCHIVE Valéry, « Ransomware : la transparence toujours relative des collectivités territoriales », LeMagIT, 29 septembre 2022. www.lemagit.fr/

ROBERTS Huw et al., « Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models », Digital Government: Research and Practice, vol. 3, n° 4, 2022.

ROBINSON Nick, Kask Laura et Krimmer Robert, « The Estonian Data Embassy and the Applicability of the Vienna Convention: A Thought Experiment », 2021.

RUTUJA Gurav, HET Patel, ZHUOCHENG Shang et al., « Can SAM recognize crops? Quantifying the zero-shot performance of a foundation model for geo-spatial tasks », International Journal of Applied Earth Observation and Geoinformation, 2024.

SAMET Hanan., « Spatial data structures »., 1995.

SCASSA Teresa, « Law enforcement in the age of big data and surveillance intermediaries : Transparency challenges ». SCRIPT-Ed, n° 14, 2017, pp. 239–284 https://www.researchgate.net/publication/321823204_Law_Enforcement_in_the_Age_of_Big_Data_and_Surveillance_Intermediaries_Transparency_Challenges

SCHMITT Michael N. et VIHUL Liis (dir), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017

SCHMIDT Susanne K., WERLE Raymund, Coordinating Technology : Studies in the International Standardization of Telecommunications, Cambridge (MA), MIT Press, 1998, p. 15.

SCHOTT Lennart et Schaefer Kerstin J., « Acceptance of Chinese latecomers' technological contributions in international standardization: Evidence from ISO and IEC », Research Policy, 2023.

SCHROTTER Gerhard et Hürzeler Christian, « The Digital Twin of the City of Zurich for Urban Planning », pp. 99-112, Springer, 2020.

SCOTT Greg et RAJABIFARD Abbas, « Sustainable development and geospatial information : a strategic framework for integrating a global policy agenda into national geospatial capabilities », Geo-

spatial Information Science, vol. 20, n° 2, 2017. https://www.tandfonline.com/doi/full/10.1080/10095020.2017.1325594

SEAMN John, « China and the New Geopolitics of Technical Standardization », Ifri, 2020, p.7. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/seaman_china_standardization_2020.pdf

SEGRESTIN Denis, « L'entreprise à l'épreuve des normes de marché. Les paradoxes des nouveaux standards de gestion dans l'industrie », Revue française de sociologie, vol. 38, 1997, pp. 38 – 39.

SEUNGHUN Kang, « Use Case of National Digital Twin Standard for Buildings », FIG Working Week 2021, 2021.

SHANE M. Greenstein, « Invisible Hands and Visible Advisors : An Economic Interpretation of Standardization. », Journal of the American Society for Information Science, n° 43, septembre 1992.

HARLEY John Brian, « Deconstructing the Map », Cartographica, vol. 26, n° 2, 1989, pp. 1-20.

SHEKHAR Aiyar, Jiaqian Chen, Christian Ebeke et al., « Geoeconomic Fragmentation and the Future of Multilateralism », International Monetary Fund, Staff Discussion Note, janvier 2023, p. 10.

SHORE Peter, « Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer », Proceedings of the 35th Annual Symposium on Foundations of computer Science, Santa Fe, NM, Nov. 20 — 22, 1994. . https://arxiv.org/abs/quant-ph/9508027

SIEBER Renee E., et Johnson Peter A., « Civic open data at a crossroads : Dominant models and current challenges », Government Information Quarterly, n° 32, 2015, pp. 308–315. https://www.researchgate.net/publication/278161820_Civic_open_data_at_a_crossroads_Dominant_models_and_current_challenges.

SIMCOE Timothy, « Standard Setting Committees : Consensus Governance for Shared Technology Platforms », American Economic Review, vol. 102, n° 1, 2012, pp. 305-336.

SIMPSON Ilona, « The Security Implications of A Digital Twin », Netskope, janvier 2024. https://www.netskope.com.

SINGH Vikram Jeet, & Bhatia Kalindhi, « India : What's driving data localisation In India? », 2020, BTG Legal. https://www.mondaq.com/india/data-protection/928916/whats-driving-data-localisation-in-india.

SNCF, « SNCF Réseau leader dans le BIM et le jumeau numérique du système ferroviaire », SNCF Numérique, 6 décembre 2022.

SOLMS (Von) R. et NIEKERK (Van) J., « From information security to cyber security. », Computers & security, n° 38, pp. 97-102, 2013.

SOLYMOSI Reka, Buil-Gil David, Ceccato Vania, Kim Eon et Jansson Ulf, « Privacy challenges in geodata and open data », GI_Forum, vol. 2, 2022, pp. 33-45.

SPAK Ulrik, « The common operational picture: A powerful enabler or a cause of severe misunderstanding? », 22nd ICCRTS, Santa Monica (CA), 2017.

SPRIVAL Andris, « Geographic Support Requirements For Future NATO Joint Expeditionary Missions », Estonian Journal of Military Studies, Volume 1, 2016, pp. 11–40, p. 3. . https://www.ksk.edu.ee/wp-content/uploads/2016/02/S%C3%B5jateadlane_1_02_Sprivul.pdf

SPRIVUL Andris, « Geographic support requirements for future NATO joint expeditionary missions », Kaitseväe Akadeemia, 2016.

Standard CNIG, « Accessibilité du cheminement en voirie : Collecte des données sur l'accessibilité du cheminement pour les personnes en situation de handicap », (v2021 - rev. Février 2024), 2024, p. 4.

STANLEY M. Besen et Farrell Joseph, « Choosing How to Compete : Strategies and Tactics in Standardization », Journal of Economic Perspectives, n° 8, 1994, pp. 117 – 131.

STAR Susan Leigh, « The Ethnography of Infrastructure », American Behavioral Scientist, vol. 43, n° 3, 1999, pp. 377-391.

Statuts du groupe AFNOR, Article 10, 10 décembre 2009.

STEVENS W. R., « TCP/IP Illustrated : The Protocols », AddisonWesley Professional, 1994.

SUBRA Philippe, Géopolitique locale. Territoires, acteurs, conflits, Armand Colin, 2016.

SYLVAIN Biget, « Guerre en Ukraine : Kropyva, l'application Android utilisée par les artilleurs ukrainiens », Futura-Science, 2022. https://www.futura-sciences.com/tech/actualites/guerre-futur-guerre-ukraine-kropyva-application-android-utilisee-artilleurs-ukrainiens-99045/

Tax Foundation, « Trump Tariffs: Tracking the Economic Impact of the Trump Trade War », 3 avril 2025. https://taxfoundation.org.

TATE Jay, « National Varieties of Standardization », in Hall Peter A. et Soskice David (dir)., Varities of Capitalism : The Institunal Foundations of Comparative Advantage, Oxford, Oxford University Press, 2011.

TAYLOR Linnet., « Public actors without public values : Legitimacy, domination and the regulation of the technology sector », Philosophy & Technology, n° 34, 2021, pp. 897–922 https://link.springer.com/article/10.1007/s13347-020-00441-4.

TEICHMANN Friedrich, « Current Technological Challenges and Innovative Approaches for Military Geo-Services from an Austrian Perspective », in Military Geoscience : A Multifaceted Approach to the Study of Warfare, Advances in Military Geosciences, Springer Nature Switzerland, 2022.

TELEANU Sorina, « The geopolitics of digital standards : China's role in standard-setting organisations », DiploFoundation/Geneva Internet Platform and Multilateral Dialogue Konrad Adenauer Foundation Geneva, 2021, p.5. https://www.diplomacy.edu/wp-content/uploads/2021/12/Geopolitics-of-digital-standards-Dec-2021.pdf

TEUFERT John F., « The NATO Core Geographic Services System : Enterprise GIS for Defense Provides Strong, Centralized Geospatial Capabilities », Esri, 2014.

TERRIOU Louis, « Estonie : la société numérique la plus avancée du monde ? », Regard sur l'Est, 11 avril 2023

THALES, « Thales et LuxCarta s'associent dans le renseignement militaire optimisé par une intelligence artificielle », 2022. https://www.thalesgroup.com.

The Economist, « Why are so many Russian generals dying in Ukraine? », 31 mars 2022.

The European Engineering Industries Association, « Speaking For European Engineering : Annual Report 2010 / 2011 », ORGALIME, 2011, p. 21.

The Geospatial-Intelligence Standards Working Group (GWG), « Geospatial Intelligence standard : Part 2 : Overview of GEOINT Standards », On-line training modules sponsored by the Geospatial Intelligence Standards Working Group (GWG), 30 janvier 2007.

The Republic of Moldova Trade Diagnostic Study, World Bank, Report No. 30998-MD, 2004.

The Times, « Uber-style technology helped Ukraine to destroy Russian battalion », mai 2022.

THIBAULT Fouillet, « Quelle place pour le cyber dans la manœuvre aéroterrestre ? », DEFTECH, n° 3, octobre-décembre 2022.

THORSBY, Jeffrey., Stowers, Genie N. L., Wolslegel, Kristen, et Tumbuan, Ellie, « Understanding the content and features of open data portals in American cities », Government Information Quarterly, n° 34, 2017, pp. 53–61.

TIMMERS Paul, « Géopolitique de la normalisation », EU Cyber Direct, 9 avril 2020. https://eucyberdirect.eu.

TOFFALETTI, S., « European SMEs and Standards« , ASTM Standardization News, 2016.

TRANBERG Pernille, « Open Source – One Path to Digital Sovereignty », Data Ethics, 28 juin 2024. https://dataethics.eu.

TROISPOUX Gilles, « La qualité des données géographiques, état des lieux pour un débat », Certu, 29 octobre 2010.

U.S Army Techniques Publication No. 3-34.80, « GEOSPATIAL ENGINEERING », Headquarters Department of the Army, Washington, DC, 22 février 2017.

UN GGIM, « Future trends in geospatial information management : the five to ten year vision », 2021, p. 23. https://ggim.un.org/meetings/GGIM-committee/10th-Session/documents/Future_Trends_Report_THIRD_EDITION_digital_accessible.pdf

UN-GGIM-AP, « Regional Workshop for Promoting the Asia-Pacific Geospatial Information Platform », 16 octobre 2020.

UNESCO, « Recommandation sur l'éthique de l'intelligence artificielle », 2021. https://www.unesco.org/fr/legal-affairs/recommendation-ethics-artificial-intelligence

Union Africaine, « Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel », 23e session ordinaire de la conférence de l'Union, Malabo, 27 juin 2014. . https://www.afapdp.org/wp-content/uploads/2018/06/CONV-UA-CYBER-PDP-2014.pdf

Groupe AFNOR, Statuts du groupe AFNOR, Article 9, 10 décembre 2009.

United States Trade Representative, « 2019 Report to Congress On China's WTO Compliance », mars 2020.

US Army, PEO IEW&S Integration Directorate, « ISA Introductory Guide », n° 6, 31 octobre 2023.

US Army, PEO IEW&S Integration Directorate, « ISA Whitepaper », Document n° 6.0, Revision n° 2, 31 octobre 2023.

USGIF, « Is Quantum Computing Poised to Transform GEOINT? », 11 avril 2024. https://usgif.org.

VACHOT Isora, « Intégrité, Confidentialité, Disponibilité : définitions », Cybersecura, 26 avril 2024. https://www.cybersecura.fr.

VALERY Tayo Tene Christian, Yuriev Alexander et Boiral Olivier, « Adopting ISO Management Standards in Africa : Barriers and Cultural Challenges », in Heras-Saizarbitoria, I. (eds.) ISO 9001, ISO 14001, and New Management Standards., Measuring Operations Performance., Springer, Cham. https://doi.org/10.1007/978-3-319-65675-5

VANCAUWENBERGHE, G., Valečkaitė, K., Van Loenen, B., et Donker, F., « Assessing the openness of spatial data infrastructures (SDI) : Towards a map of open SDI », in International Journal of Spatial Data Infrastructures Research, n°13, 2018, pp. 88–100. https://www.researchgate.net/publication/323521479_Assessing_the_Openness_of_Spatial_Data_Infrastructures_SDI_Towards_a_Map_of_Open_SDI

VERDIER Amelle, « La portée juridique de l'information géospatiale dans la jurisprudence administrative et civile », Afigéo, mars 2019.

VILA Seoane, M. F., « Data sécurisation : the challenges of data sovereignty in India », in Third World Quarterly, 42(8), 2021, pp. 1733–1750. https://doi.org/10.1080/01436597.2021.1915122

VINEN Richard, « Politics of French Business, 1936-1945. », New York, Cambridge University Press, 1991.

VISHAL Rana et Govand Khalid Azeez, « Southeast Asia's Quest for Digital Sovereignty », in The Diplomat, 19 mars 2025. . Consulté le 19 mai 2025. https://thediplomat.com/2025/03/southeast-asias-quest-for-digital-sovereignty/

VON Hayek Friedrich, Droit, législation et liberté, vol. 3 : L'ordre politique d'un peuple libre, Paris, PUF, 1983.

WANG Ping et LIANG Zheng, « Beyond Government Control of China's Standardization System -- History, Current Status and Reform Suggestions », 27 janvier 2016.

WEBER Max, « Économie et société », tome 1, Paris, Plon, 1995.

WEBER Max, « Le savant et le politique » in « La politique comme profession et vocation », Paris, La Découverte, p. 118, 2003.

WHALEN Jeanne, « Government Should Take Bigger Role in Promoting U.S. Technology or Risk Losing Ground to China, Commission Warns », The Washington Post, 2021.

WINNER Langdon, « Do Artifacts Have Politics? », Daedalus, vol. 109, n° 1, 1980, pp. 121-136.

WITHINGTON Thomas, « DesertStorm30 – Electric Avenue : Electronic Warfare and the battle against Iraq's air defences during Operation Desert Storm », in Air Power History, 20 janvier 2022. https://balloonstodrones.com/2022/01/20/desertstorm30-electric-avenue-electronic-warfare-and-the-battle-against-iraqs-air-defences-during-operation-desert-storm/

WOOD Denis, FELS John, The Power of Maps, New York, Guilford Press, 1992.

XINFENG Ye et Lei Zhong, « Improving web service security and privacy »., In 2011 IEEE World Congress on Services, pp. 406–413. IEEE, 2011.

XIRIU Li, « Southeast Asia’s Data Localization Push Is a Double-Edged Sword », in The Diplomat, 28 octobre 2022. . Consulté le 12 mars 2025. https://thediplomat.com/2022/10/southeast-asias-data-localization-push-is-a-double-edged-sword/

YONGMING Xu, Benjamin Lewis et Weihe Wendy Guan, « Developing the Chinese Academic Map Publishing Platform », in Spatial Literary Studies in China, Geocriticism and Spatial Literary Studies, Palgrave Macmillan, Cham, 2022, p 53 – 80. https://link.springer.com/chapter/10.1007/978-3-031-03914-0

ZANDBERGEN P. A., « Ensuring Confidentiality of Geocoded Health Data : Assessing Geographic Masking Strategies for Individual-Level Data », Advances in Medicine, 2014.

ZHANG Ketian, « Alliances with Chinese characteristics? The contents and rationale of China’s strategic partnerships », in International Politics, Vol. 62(2), Palgrave Macmillan, 2 juin 2025. https://link.springer.com/article/10.1057/s41311-025-00701-0

ZHANG M. et al., « Geomasking to Safeguard Geoprivacy in Geospatial Health Data », Encyclopedia, vol. 4, n° 4, 2024, p. 103.

ZOOK Matthew, Graham Mark, Shelton Taylor et Gorman Sean., « Volunteered geographic information and crowdsourcing disaster relief : A case study of the Haitian earthquake », World Medical & Health Policy, n°2, 2012, pp. 6–32. https://onlinelibrary.wiley.com/doi/10.2202/1948-4682.1069

ZOPE-CHAUDHARI Sangita et Venkatachalam P, « Conceptual framework for geospatial data security », International Journal of Database Management Systems, n° 5, p. 29, 2013.

ZUNIGA Nicholas , BURTON Datta Saheli , BLANCATO Filippo, CARR Madeline, « The geopolitics of technology standards : historical context for US, EU and Chinese approaches », in International Affairs, Vol. 100, n°4, Juillet 2024, pp. 1635–1652. https://academic.oup.com/ia/article/100/4/1635/7692873

TABLE DES FIGURES ET TABLEAUX

Liste des figures

Numéro	Titre	Localisation
Figure 1	Diagramme du modèle OSI	Cadre théorique
Figure 2	La normalisation internationale en France et dans le monde	Chapitre I
Carte 1	Implantation mondiale du groupe AFNOR (2025)	Chapitre I
Figure 3	Architecture du système français de normalisation	Chapitre I
Figure 4	Processus d’adoption d’une norme internationale ISO	Chapitre I
Figure 5	Architecture des normes OGC	Chapitre II
Figure 6	Évolutions de la législation européenne concernant la protection des données	Chapitre II
Figure 7	Évolution du système de normalisation chinois : comparaison des structures jusqu'en 2017 et après 2018	Chapitre II
Carte 2	Modèles nationaux d'organisation de la normalisation géospatiale	Chapitre II
Figure 8	Répartition des groupes de travail de l’ISO/TC 211	Chapitre II

Carte 3	Pays participants à la normalisation géospatiale mondiale	Chapitre II
Figure 9	Structure du DGIWG	Chapitre II
Carte 4	Pays membres de l’OTAN	Chapitre II
Figure 10	Évolution prévisionnelle des recettes (programmes coproduction)	Chapitre III
Figure 11	Architecture de production de données géographiques (armées)	Chapitre III
Figure 12	Principales opérations des armées françaises	Chapitre III
Figure 13	Catégories de savoirs fusionnés dans le cadre du GEOINT	Chapitre III
Figure 14	Les services Web OGC	Chapitre IV
Figure 15	Organisation du CNIG	Chapitre V
Figure 16	Liste des normes validées par le CNIG	Chapitre V
Figure 17	Liste des projets de normes en préparation au sein du CNIG	Chapitre V
Carte 5	Acteurs de l’information géographique dans les territoires étudiés	Chapitre VI
Carte 6	Avancement des	Chapitre VI

	acquisitions LIDAR HD	
Carte 7	Avancement de l’OCS GE	Chapitre VI
Figure 18	Architecture du Jumeau Numérique France et des Territoires (JNFT)	Chapitre VI
Carte 8	Le poids normatif des nations au sein de l’ISO/TC 211 (2024)	Chapitre VII

Liste des tableaux

Numéro	Titre	Localisation
Tableau 1	Corpus d'entretiens semi-directifs	Cadre méthodologique
Tableau 2	Répartition institutionnelle des entretiens	Cadre méthodologique
Tableau 3	Synthèse des observations participantes par niveau scalaire	Cadre méthodologique

Note : *La numérotation des figures suit l'ordre d'apparition dans le manuscrit. Les tableaux du cadre méthodologique sont numérotés séparément des tableaux présents dans les annexes.*

ANNEXES — Enquête de terrain : entretiens et observations

Les transcriptions ne sont pas présentes dans la version de diffusion pour des raisons de confidentialité.

Annexe B — Tableau récapitulatif des observations participantes

Cette annexe présente une synthèse des observations participantes réalisées dans le cadre de l'enquête de terrain (mars 2022 – décembre 2023). Les notes d'observation complètes sont disponibles en annexe numérique.

B1. Synthèse des observations par échelle

Échelle	Instances observées	Nb réunions	Période
Nationale (CNIG)	Commissions, GT, Pôles, Plénières	33	Mai 2022 – Déc. 2023
Défense / OTAN	MGCP, TREx, MUVD, IPHG	28	Oct. 2022 – Déc. 2023
Internationale civile	ISO/TC 211 (WG1, WG6, WG7, WG9, WG10...)	30	Déc. 2022 – Oct. 2023
Internationale défense	DGIWG, SIFWG	23	Janv. 2023 – Nov. 2023
TOTAL		**114**	**Mars 2022 – Déc. 2023**

Source : Enquête de terrain, 2022-2023.

B2. Réunions observées — Échelle nationale (CNIG)

Sélection de 12 réunions sur 33 observées.

Date	Instance / Thème	Type	Lieu
09/05/2022	Commission des Standards	Commission	Paris
16/06/2022	GT Risques	GT	Visio
23/06/2022	GT DDU (Documents d'urbanisme)	GT	Visio
24/06/2022	GT Bâti	GT	Visio
07/09/2022	Pôle Coordination des Territoires	Pôle	Visio
26/09/2022	Commission Modèles Économiques	Commission	Paris
06/10/2022	GT DOMES (identifiants stations)	GT	Visio
10/11/2022	Comité des Standards	Commission	Paris
02/12/2022	Conseil plénier	Plénière	Paris
19/01/2023	Commission des Standards	Commission	Paris
01/06/2023	Commission des Standards	Commission	Paris
14/12/2023	Commission des Standards	Commission	Paris

B3. Réunions observées — Échelle Défense / OTAN

Sélection de 9 réunions sur 28 observées.

Date	Instance / Thème	Type	Lieu
04-05/10/2022	Programme IPHG	Réunion	Paris
14-15/11/2022	Programme MGCP	Réunion	Paris
22/11/2022	Programme MUVD	Réunion	Paris
30/11/2022	Programme TREx	Réunion	Paris
25/04/2023	TREx – 19e plénière	Plénière	Strasbourg
26-27/04/2023	MGCP – 41e plénière	Plénière	Strasbourg
28/04/2023	MUVD – 6e plénière	Plénière	Strasbourg

25-29/09/2023	MGCP TG45	GT	Strasbourg
04-05/10/2023	IPHG TG13	GT	Saint-Mandé

B4. Réunions observées — Échelle internationale civile (ISO/TC 211)

Sélection de 10 réunions sur 30 observées.

Date	Instance / Thème	Type	Lieu
05/12/2022	57e réunion WG7	GT	Stockholm
06/12/2022	23e réunion WG10	GT	Stockholm
07/12/2022	Standards in Action Seminar	Séminaire	Stockholm
08/12/2022	Program Maintenance Group	Réunion	Stockholm
04/01/2023	27e réunion WG1	GT	Visio
22/02/2023	60e réunion WG7	GT	Visio
15/05/2023	32e réunion WG6 – Imagerie	GT	Jeonju (Corée)
15/05/2023	65e réunion WG7	GT	Jeonju (Corée)
17/05/2023	Standards in Action Seminar	Séminaire	Jeonju (Corée)
18-19/05/2023	Plénière ISO/TC 211	Plénière	Jeonju (Corée)

B5. Réunions observées — Échelle internationale défense (DGIWG)

Sélection de 6 réunions sur 23 observées.

Date	Instance / Thème	Type	Lieu
20/01/2023	Geospatial Web Service Program	GT	Visio
06-09/03/2023	WSTP Meeting (P5)	GT	Munich
17-20/04/2023	WSTP Meeting (P5)	GT	Pont-à-Mousson
24/04/2023	Plénière conjointe DGIWG/MGCP/OGC	Plénière	Strasbourg
23-27/10/2023	DGIWG Plenary Meeting	Plénière	Garmisch
28/11/2023	Joint Meeting DGIWG/SIFWG	Réunion	Visio

B6. Notes méthodologiques

Confidentialité : Certaines réunions observées dans le cadre des programmes de coproduction (MGCP, TREx, MUVD, IPHG) et des instances DGIWG peuvent contenir des informations à diffusion restreinte. Les notes d'observation seront anonymisées conformément aux règles en vigueur si elles sont demandées.

Annexe numérique : Les notes d'observation complètes (153 entrées) sont disponibles sur demande auprès de l'auteur. Elles comprennent les comptes rendus détaillés des réunions, les échanges informels documentés et les observations sur les dynamiques d'interaction entre délégations.

Codification : Les codes utilisés dans cette annexe (E01-E25 pour les entretiens) permettent de référencer les sources dans le corps de la thèse.

Annexe C — Glossaire des sigles et acronymes

Ce glossaire recense les principaux sigles et acronymes utilisés dans cette thèse, classés par ordre alphabétique. Les termes sont regroupés en plusieurs domaines : organisations de normalisation, institutions de défense, programmes géospatiaux, normes et standards techniques, technologies informatiques et cybersécurité.

Sigle / Acronyme	Signification
A	
AES	Advanced Encryption Standard
AFNOR	Association française de normalisation
AG	Advisory Group (Groupe consultatif, ISO/TC 211)
AML	Additional Military Layers (Couches militaires additionnelles)
ANSI	American National Standards Institute (Institut américain de normalisation)
ANSSI	Agence nationale de la sécurité des systèmes d'information
API	Application Programming Interface (Interface de programmation)
APREF	Asia-Pacific Reference Frame
ASEAN	Association of Southeast Asian Nations (Association des nations de l'Asie du Sud-Est)
AWS	Amazon Web Services

B	
BGHOM	Bureau géographie, hydrographie, océanographie et météorologie (ministère des Armées)
BIM	Building Information Modeling (Modélisation des informations du bâtiment)
BSI	British Standards Institute (Institut britannique de normalisation)
C	
CCDCOE	Cooperative Cyber Defence Centre of Excellence (OTAN, Tallinn)
CCPN	Comité de coordination et de pilotage de la normalisation
CEN	Comité européen de normalisation
CENELEC	Comité européen de normalisation électrotechnique
CERT	Computer Emergency Response Team
CityGML	City Geography Markup Language
CN	Commission de normalisation
CNIG	Conseil national de l'information géolocalisée (anciennement géographique)
CNIL	Commission nationale de l'informatique et des libertés
COVADIS	Commission de validation des données pour l'information spatialisée
CRAIG	Centre régional Auvergne-Rhône-Alpes de l'information géographique
CRIGE	Centre régional de l'information géographique
CT	Comité technique
CWIX	Coalition Warrior Interoperability eXercise (exercice OTAN)
D	
DCAT	Data Catalog Vocabulary
DDT	Direction départementale des territoires
DEAL	Direction de l'environnement, de l'aménagement et du logement (outre-mer)
DGA	Direction générale de l'armement

DGALN	Direction générale de l'aménagement, du logement et de la nature
DGIF	Defence Geospatial Information Framework (Cadre d'information géospatiale de défense)
DGIWG	Defence Geospatial Information Working Group (Groupe de travail sur l'information géospatiale de défense)
DGSE	Direction générale de la sécurité extérieure
DIN	Deutsches Institut für Normung (Institut allemand de normalisation)
DREAL	Direction régionale de l'environnement, de l'aménagement et du logement
E	
EDR	Environnement Data Retrieval
ENISA	European Union Agency for Cybersecurity (Agence de l'UE pour la cybersécurité)
EPCI	Établissement public de coopération intercommunale
ESA	European Space Agency (Agence spatiale européenne)
ESRI	Environmental Systems Research Institute
ETSI	European Telecommunications Standards Institute (Institut européen des normes de télécommunications)
G	
GAFAM	Google, Apple, Facebook (Meta), Amazon, Microsoft
GEOCAPI	Géographie capacitaire interarmées
GEODE 4D	Programme de modernisation des systèmes d'information géographique de défense
GEOINT	Geospatial Intelligence (Renseignement géospatial)
GeoJSON	Geographic JavaScript Object Notation
GeoPackage	Format de conteneur géospatial ouvert (OGC)
GeoSPARQL	Geographic SPARQL Protocol and RDF Query Language
GeoTIFF	Geographic Tagged Image File Format
GIP	Groupement d'intérêt public

GLONASS	Global Navigation Satellite System (système russe)
GML	Geography Markup Language (Langage de balisage géographique)
GNSS	Global Navigation Satellite System (Système mondial de navigation par satellite)
GPS	Global Positioning System (Système de positionnement mondial)
GT	Groupe de travail
GWG	Geospatial-Intelligence Working Group (USA)
H	
HTTP / HTTPS	HyperText Transfer Protocol / Secure
I	
IA / AI	Intelligence artificielle / Artificial Intelligence
IDS	Infrastructure de données spatiales
IDSA	International Data Spaces Association
IEC / CEI	International Electrotechnical Commission / Commission électrotechnique internationale
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGN	Institut national de l'information géographique et forestière
IHO / OHI	International Hydrographic Organization / Organisation hydrographique internationale
INSEE	Institut national de la statistique et des études économiques
INSPIRE	Infrastructure for Spatial Information in the European Community
IP	Internet Protocol
IPHG	International Program for Human Geography (Programme international de géographie humaine)
ISO	International Organization for Standardization (Organisation internationale de normalisation)
ISO/TC 211	Comité technique 211 de l'ISO — Informations géographiques / Géomatique

ITU / UIT	International Telecommunication Union / Union internationale des télécommunications
J	
JNFT	Jumeau numérique de la France et des Territoires
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
JTC 1	Joint Technical Committee 1 (Comité technique mixte ISO/IEC pour les technologies de l'information)
K	
KML	Keyhole Markup Language
L	
LADM	Land Administration Domain Model (Modèle du domaine de l'administration des terres)
LIDAR	Light Detection and Ranging (Détection et télémétrie par la lumière)
M	
MASINT	Measurement and Signature Intelligence
MGCP	Multinational Geospatial Co-production Program (Programme multinational de coproduction géospatiale)
MNT	Modèle numérique de terrain
MUVD	Multinational Urban Vector Data (Données vecteur urbaines multinationales)
N	
NCIA	NATO Communications and Information Agency
NGA	National Geospatial-Intelligence Agency (États-Unis)
NGIF	NATO Geospatial Information Framework
NIS / NIS2	Network and Information Security (directive européenne)
NIST	National Institute of Standards and Technology (Institut américain des normes et technologies)

NSA	National Security Agency (États-Unis)
NWIP	New Work Item Proposal (Proposition de nouveau sujet de travail, ISO)
O	
OASIS	Organization for the Advancement of Structured Information Standards
OCDE	Organisation de coopération et de développement économiques
OCS GE	Occupation du sol à grande échelle
OGC	Open Geospatial Consortium
OMC	Organisation mondiale du commerce
ONU	Organisation des Nations unies
OSI	Open Systems Interconnection (modèle de référence)
OSM	OpenStreetMap
OTAN / NATO	Organisation du traité de l'Atlantique Nord / North Atlantic Treaty Organization
OVH	Société française d'hébergement et de services cloud
OWL	Web Ontology Language
P	
PCRS	Plan de corps de rue simplifié
PME	Petites et moyennes entreprises
PQC	Post-Quantum Cryptography (Cryptographie post-quantique)
Q	
QKD	Quantum Key Distribution (Distribution quantique de clés)
R	
RDF	Resource Description Framework
REST	Representational State Transfer
RGE	Référentiel à grande échelle
RGPD	Règlement général sur la protection des données
RSA	Rivest-Shamir-Adleman (algorithme de chiffrement)
RSSI	Responsable de la sécurité des systèmes d'information

S	
S-100	Modèle universel de données hydrographiques de l'OHI
SAC	Standardization Administration of China (Administration chinoise de normalisation)
SAR	Synthetic Aperture Radar (Radar à synthèse d'ouverture)
SC	Sous-comité
SHOM	Service hydrographique et océanographique de la marine
SIFWG	Sensor Integration Framework Working Group
SIG / GIS	Système d'information géographique / Geographic Information System
SOC	Security Operations Center
SQL	Structured Query Language
SSI	Sécurité des systèmes d'information
STANAG	Standardization Agreement (Accord de normalisation OTAN)
T	
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TMB	Technical Management Board (Bureau de gestion technique de l'ISO)
TPE	Très petites entreprises
TR	Technical Report (Rapport technique)
TREx	TanDEM-X High Resolution Elevation Data Exchange
TS	Technical Specification (Spécification technique)
U	
UE	Union européenne
UNESCO	Organisation des Nations unies pour l'éducation, la science et la culture
UN-GGIM	United Nations Committee of Experts on Global Geospatial Information Management
URL	Uniform Resource Locator
V	

VMAP	Vector Map (Carte vecteur)
W	
W3C	World Wide Web Consortium
WAF	Web Application Firewall
WCS	Web Coverage Service
WFS	Web Feature Service (Service d'accès aux entités géographiques)
WG	Working Group (Groupe de travail)
WMS	Web Map Service (Service de cartes web)
WMTS	Web Map Tile Service
WPS	Web Processing Service
X	
XML	Extensible Markup Language

Annexe D — Grille d'entretien semi-directif

Cette annexe présente la grille d'entretien utilisée pour les vingt-cinq entretiens semi-directifs conduits entre mars 2022 et juin 2023. La grille est organisée autour de cinq axes thématiques et a été adaptée en fonction du profil de chaque enquêté.

D1. Grille d'entretien type

Axe 1 — Parcours professionnel et positionnement institutionnel

Objectif : *Contextualiser le discours de l'enquêté et comprendre sa position dans le champ de l'information géographique*

Questions indicatives :

- Pouvez-vous me présenter votre parcours professionnel et votre rôle actuel au sein de votre institution ?
- Depuis combien de temps travaillez-vous dans le domaine de l'information géographique ?
- Quelle est la place de l'information géographique dans les missions de votre organisation ?
- Comment êtes-vous amené(e) à interagir avec les processus de normalisation (national, européen, international) ?

Axe 2 — Pratiques de production et de gestion des données géographiques

Objectif : *Saisir les pratiques concrètes, les normes suivies et les difficultés rencontrées*

Questions indicatives :

- Quels types de données géographiques produisez-vous ou utilisez-vous dans votre activité quotidienne ?
- Quels formats et standards utilisez-vous pour la production et l'échange de données (ISO 19115, GML, GeoPackage, etc.) ?
- Comment choisissez-vous les normes à appliquer ? Ce choix est-il contraint ou libre ?
- Rencontrez-vous des difficultés liées à l'interopérabilité des données avec d'autres acteurs ?
- Avez-vous dû faire des arbitrages entre différentes normes ou formats ? Lesquels et pourquoi ?

Axe 3 — Relations avec l'écosystème de l'information géographique

Objectif : *Explorer les modalités de coopération et les éventuelles tensions entre acteurs*

Questions indicatives :

- Avec quels acteurs de l'écosystème de l'information géographique êtes-vous en relation (IGN, CNIG, collectivités, plateformes régionales, organisations internationales) ?
- Comment qualifieriez-vous ces relations : coopération, complémentarité, concurrence, tension ?
- Participez-vous aux travaux de normalisation (CNIG, AFNOR, ISO/TC 211, OGC, DGIWG) ? Si oui, comment et à quel titre ?
- Avez-vous le sentiment que les intérêts de votre organisation sont bien représentés dans les instances de normalisation ?
- Percevez-vous des rapports de force entre acteurs dans les processus de normalisation ? Pouvez-vous donner des exemples ?

Axe 4 — Cybersécurité et protection des données géographiques

Objectif : *Évaluer la perception des menaces, les mesures mises en œuvre et les incidents éventuels*

Questions indicatives :

- Les données géographiques que vous manipulez présentent-elles des enjeux de sécurité ou de confidentialité ?
- Votre organisation a-t-elle été confrontée à des incidents de cybersécurité impliquant des données géographiques ?
- Quelles mesures de protection avez-vous mises en place (chiffrement, contrôle d'accès, audits, etc.) ?
- Considérez-vous que les normes actuelles intègrent suffisamment les exigences de cybersécurité ?
- Avez-vous connaissance de standards spécifiques à la sécurité des données géospatiales (OGC WSS, GeoXACML, S-100 chapitre 15) ?

Axe 5 — Souveraineté numérique et enjeux géopolitiques

Objectif : *Recueillir les représentations sur les enjeux stratégiques de la normalisation*

Questions indicatives :

- Comment définiriez-vous la notion de « souveraineté numérique » dans le contexte de l'information géographique ?
- Pensez-vous que la normalisation des données géographiques constitue un enjeu stratégique pour la France ? Pourquoi ?
- Observez-vous une évolution des rapports de force dans les instances internationales de normalisation (montée de la Chine, rivalité sino-américaine) ?

- La France et l'Europe vous semblent-elles bien positionnées pour défendre leurs intérêts dans ce domaine ?
- Quelles évolutions anticipez-vous dans les années à venir (fragmentation normative, émergence de nouveaux acteurs, impact de l'IA) ?
- Avez-vous des recommandations pour renforcer la position de la France dans l'écosystème normatif international ?

D2. Adaptations selon les profils d'acteurs

La grille type a été adaptée en fonction des catégories d'acteurs enquêtés, afin de tenir compte des spécificités de leur positionnement institutionnel et de leurs pratiques.

Acteurs de la défense (DGA, BGHOM, 28e Groupe géographique)

- Questions spécifiques sur les programmes de coproduction (MGCP, TREx, MUVD, IPHG)
- Enjeux d'interopérabilité avec les forces alliées (OTAN, DGIWG)
- Classification et protection des données géographiques militaires
- Articulation entre normes civiles (ISO) et normes militaires (STANAG)

Acteurs territoriaux (DREAL, DEAL, Régions, CRIGE)

- Focus sur les plateformes régionales d'information géographique
- Enjeux de mutualisation et de gouvernance des données locales
- Relations avec l'État central (IGN, CNIG) et les collectivités
- Impact des attaques cyber sur les infrastructures territoriales

Experts normalisation (IGN, AFNOR, délégués ISO/TC 211)

- Fonctionnement interne des comités techniques et groupes de travail
- Stratégies d'influence et de négociation dans les arènes internationales
- Évolution de la gouvernance des organisations de normalisation
- Positionnement de la France par rapport aux autres délégations

Acteurs de la cybersécurité (ANSSI)

- Articulation entre normalisation et réglementation (NIS2, RGPD)
- Référentiels de sécurité applicables aux SIG
- Menaces spécifiques aux infrastructures d'information géographique
- Coopération internationale en matière de cybersécurité

D3. Conditions de réalisation des entretiens

Durée moyenne : 1h à 2h selon les enquêtés.

Modalité : Entretiens en présentiel ou en visioconférence selon les contraintes géographiques et d’agendas.

Enregistrement : Avec l'accord préalable des personnes interrogées. Certains entretiens ont été retranscrits intégralement.

Validation : Les citations mobilisées dans le corps de la thèse ont fait l'objet, lorsque requis, d'une validation par les enquêtés.

Anonymisation : Sur demande de certains enquêtes, les propos ont été anonymisés ou attribués de manière générique (« un responsable de... »).

Annexe E — Cartographie de l'écosystème normatif géospatial

Cette annexe présente une vue synthétique de l'écosystème normatif des données géographiques numériques, structuré en quatre niveaux : international civil, européen, défense/OTAN, et national français.

F1. Acteurs de la normalisation géospatiale par niveau

International (civil)			
Acteur	**Description**	**Productions normatives**	**Rôle principal**
ISO/TC 211	Comité technique de l'ISO pour l'information géographique	Normes ISO 19100	Consensus international
OGC	Open Geospatial Consortium	Standards ouverts (WMS, WFS, GML, API)	Innovation, interopérabilité
W3C	World Wide Web Consortium	Standards web (JSON-LD, RDF)	Web sémantique
IHO / OHI	Organisation hydrographique internationale	Normes S-100 (données maritimes)	Navigation maritime
UN-GGIM	Comité d'experts de l'ONU sur l'information géospatiale	Cadres directeurs, IGIF	Coordination mondiale

Européen			
Acteur	**Description**	**Productions normatives**	**Rôle principal**
CEN/TC 287	Comité technique du CEN pour l'information géographique	Normes européennes (EN)	Transposition ISO, spécificités UE
INSPIRE	Infrastructure d'information géographique européenne	Directive, règlements d'implémentation	Interopérabilité UE
ETSI	Institut européen des normes de télécommunications	Normes télécom et cybersécurité	Sécurité numérique
IDSA	International Data Spaces Association	Espaces de données	Interconnexion des données

Défense / OTAN			
Acteur	**Description**	**Productions normatives**	**Rôle principal**
DGIWG	Defence Geospatial Information Working Group	Standards DGIF, DGIM, profils défense	Interopérabilité alliés
OTAN (NSO)	NATO Standardization Office	STANAG géospatiaux	Normalisation militaire
MGCP	Multinational Geospatial Co-production Program	Spécifications de production	Coproduction cartographique
TREx	TanDEM-X High Resolution Elevation Data Exchange	Échange de données altimétriques haute résolution TanDEM-X	Mutualisation données
MUVD	Multinational Urban Vector Data	Données urbaines	Théâtres urbains
IPHG	International Program for	Géographie humaine	Renseignement

	Human Geography		

National (France)			
Acteur	**Description**	**Productions normatives**	**Rôle principal**
AFNOR	Association française de normalisation	Normes NF, miroir ISO	Normalisation française
CN InfoGéo	Commission de normalisation Information géographique	Participation ISO/TC 211	Position française à l'ISO
CNIG	Conseil national de l'information géolocalisée	Standards CNIG, coordination	Politique nationale IG
IGN	Institut national de l'information géographique	Référentiels, expertise	Production, R&D
ANSSI	Agence nationale sécurité SI	Référentiels cybersécurité	Sécurité des SIG
DGA / BGHOM	Direction générale de l'armement / Bureau géographie	Besoins militaires	Expression besoins défense

E2. Principales relations entre acteurs

L'écosystème normatif est caractérisé par un réseau dense de relations formelles (accords de liaison, conventions) et informelles (participation croisée aux travaux).

- ISO/TC 211 ↔ OGC : Accord de liaison, harmonisation des normes
- ISO/TC 211 → CEN/TC 287 : Accords de Vienne (transposition automatique)
- CEN/TC 287 → INSPIRE : Normes de référence pour l'implémentation
- DGIWG → ISO/TC 211 : Profils défense basés sur normes ISO
- DGIWG ↔ OGC : Collaboration technique (services web)
- OTAN (NSO) → DGIWG : Cadrage stratégique, STANAG
- AFNOR → ISO : Représentation française, vote
- CN InfoGéo → ISO/TC 211 : Délégation française, experts
- CNIG ↔ IGN : Coordination nationale, expertise technique
- IGN → Programmes OTAN : Maîtrise d'œuvre production
- DGA/BGHOM → IGN : Expression des besoins défense

E3. Architecture multiniveau de la normalisation

L'architecture de la normalisation géospatiale peut être représentée comme une structure pyramidale à quatre niveaux interconnectés :

Niveau 1 — International civil (ISO/TC 211, OGC) : Définit les modèles conceptuels de référence, les schémas d'encodage et les services interopérables. Ce niveau structure l'ensemble de l'écosystème par son caractère fondateur.

Niveau 2 — Européen (CEN, INSPIRE) : Transpose les normes internationales avec des adaptations réglementaires propres à l'Union européenne. Crée un cadre juridique contraignant pour les États membres.

Niveau 3 — Défense (DGIWG, OTAN) : Développe des profils spécifiques aux besoins militaires tout en maintenant la compatibilité avec les normes civiles. Assure l'interopérabilité entre forces alliées.

Niveau 4 — National (AFNOR, CNIG, IGN) : Participe à l'élaboration des normes internationales, transpose et adapte au contexte national, développe des standards spécifiques (PCRS, OCS GE).

E4. Position de la France dans l'écosystème

La France occupe une position significative dans cet écosystème grâce à plusieurs atouts : une représentation active au sein de l'ISO/TC 211 (membre P, plusieurs animateurs de groupes de travail), une participation historique aux programmes de coproduction OTAN (MGCP, TREx), un institut de référence (IGN) reconnu internationalement, et une infrastructure nationale structurée autour du CNIG. Toutefois, cette position est aujourd'hui mise en danger par la montée en puissance d'autres acteurs, notamment la Chine, et par la domination croissante des standards de facto portés par les grands acteurs technologiques américains.

Annexe F — Tableau des principales normes géospatiales

Cette annexe recense les principales normes et standards techniques relatifs à l'information géographique numérique mentionnés dans cette thèse. Les normes sont organisées par organisme émetteur.

Normes ISO (série 19100 — Information géographique)

Référence	Titre	Objet	Statut
ISO 19101	Modèle de référence	Cadre conceptuel pour toutes les normes de la série	Publiée (2014)
ISO 19103	Langage de schéma conceptuel	Règles pour exprimer les modèles en UML	Publiée (2015)
ISO 19107	Schéma spatial	Modèle géométrique et topologique	Publiée (2019)
ISO 19108	Schéma temporel	Gestion de la dimension temporelle	Publiée (2002)
ISO 19109	Règles de schéma d'application	Méthodologie de modélisation	Publiée (2015)
ISO 19110	Catalogage des entités	Structure des catalogues d'objets	Publiée (2016)
ISO 19111	Système de références par coordonnées	Définition des systèmes géodésiques	Publiée (2019)
ISO 19115	Métadonnées	Description des jeux de données géographiques	Publiée (2014)
ISO 19119	Services	Architecture des services géospatiaux	Publiée (2016)
ISO 19125	Accès aux entités simples	Simple Features (géométries de base)	Publiée (2004)
ISO 19131	Spécifications de contenu	Structure des spécifications de produits	Publiée (2007)

ISO 19136	GML	Geography Markup Language (encodage XML)	Publiée (2020)
ISO 19139	Implémentation XML des métadonnées	Schémas XML pour ISO 19115	Publiée (2019)
ISO 19152	LADM	Modèle d'administration des terres	Publiée (2012)
ISO 19157	Qualité des données	Éléments et mesures de qualité	Publiée (2013)

Standards OGC (Open Geospatial Consortium)

Référence	Titre	Objet	Statut
WMS	Web Map Service	Service de diffusion de cartes (images)	v1.3.0
WFS	Web Feature Service	Service d'accès aux entités vecteurs	v2.0.2
WCS	Web Coverage Service	Service d'accès aux données maillées	v2.1
WPS	Web Processing Service	Service de géotraitement	v2.0
WMTS	Web Map Tile Service	Service de diffusion de tuiles	v1.0
CSW	Catalogue Service for the Web	Service de catalogue de métadonnées	v3.0
SensorML	Sensor Model Language	Modélisation des capteurs	v2.0
GeoPackage	GeoPackage	Format conteneur SQLite	v1.3
GeoJSON	GeoJSON	Encodage JSON des géométries	RFC 7946
OGC API Features	OGC API - Features	API REST pour entités géographiques	v1.0
CityGML	City Geography Markup Language	Modélisation 3D urbaine	v3.0
IndoorGML	Indoor GML	Modélisation d'espaces intérieurs	v1.1
GeoSPARQL	GeoSPARQL	Requêtes spatiales sur graphes RDF	v1.0
SWE	Sensor Web Enablement	Suite de standards capteurs	Multiple

Standards de défense (DGIWG, OTAN)

Référence	Titre	Objet	Statut
DGIF	Defence Geospatial Information Framework	Cadre de référence défense	Ed. 2
DGIM	Defence Geospatial Information Model	Modèle de données défense	Ed. 2
DGFCD	Defence Feature Concept Dictionary	Dictionnaire d'entités défense	Ed. 2
STANAG 2586	Profil de métadonnées OTAN	AGeoP-08 — Métadonnées géospatiales	Ed. B
STANAG 2592	Cadre NGIF	AGeoP-11 — Framework géospatial OTAN	Ed. A
STANAG 7170	Couches militaires additionnelles	AGeoP-19 — AML	Ed. B
STANAG 2211	Datums et projections	AGeoP-21 — Références géodésiques	Ed. A
STANAG 6523	Services web défense	AGeoP-26 — Web services géospatiaux	Ed. A
STANAG 2215	Évaluation des cartes	Qualité des produits cartographiques	Ed. 7
STANAG 1059	Codes géographiques	Codes lettres des entités géographiques	Ed. 8

Standards hydrographiques (OHI / IHO)

Référence	Titre	Objet	Statut
S-100	Modèle universel hydrographique	Framework pour tous les produits IHO	Ed. 5.0
S-101	Spécification ENC	Cartes électroniques de navigation	Ed. 1.1
S-102	MNT bathymétrique	Modèle numérique de terrain sous-marin	Ed. 2.2

S-104	Niveaux d'eau	Prédictions de marées et niveaux	Ed. 1.0
S-111	Courants de surface	Données de courants marins	Ed. 1.1
S-57	Format ENC historique	Format de transfert (en remplacement)	Ed. 3.1
S-63	Protection des données	Schéma de chiffrement IHO	Ed. 1.2

Standards nationaux (CNIG France)

Référence	Titre	Objet	Statut
PCRS	Plan de corps de rue simplifié	Référentiel très grande échelle	v2.0
OCS GE	Occupation du sol grande échelle	Classification occupation des sols	v2.0
GraceTHD	Aménagement numérique territoires	Réseaux télécoms (fibre)	v3.0
DDU	Documents d'urbanisme	Dématérialisation PLU/SCOT	v2022
Risques	Données risques naturels	Plans de prévention	v2021
Accessibilité	Cheminements PMR	Accessibilité voirie	v2021
BAN	Base adresse nationale	Référentiel d'adresses	Spéc. CNIG

Notes :

- Les statuts indiqués correspondent à la situation au moment de la rédaction de la thèse (2023-2024).
- Les normes ISO de la série 19100 sont régulièrement révisées. Il faut consulter le site de l'ISO pour connaître les versions en vigueur.
- Les standards OGC évoluent rapidement. La transition vers les OGC API est en cours.
- L'accès aux STANAG peut être restreint. Seuls les documents publics sont référencés.

Table des matières

Remerciements....6
Introduction....8
Cadre théorique et méthodologique....13
1. Ancrage géopolitique : de l'espace physique au cyberespace....13
1.1. La géopolitique comme étude des rivalités de pouvoir sur les territoires....13
1.2. L'extension de la géopolitique au cyberespace....14
1.3. La norme comme territoire : vers une géopolitique des espaces normatifs....15
2. La souveraineté numérique : clarification conceptuelle....16
2.1. La souveraineté : un concept polysémique....16
2.2. Trois conceptions de la souveraineté numérique....17
2.3. Définition retenue pour la présente recherche....18
3. L'économie politique de la normalisation : cadre analytique....19
3.1. La normalisation comme gouvernance privée transnationale....19
3.2. La norme comme « dispositif cognitif collectif »....20
3.3. Effets de réseau, rendements croissants et dépendance normative....21
3.4. Les « batailles de standards » et leurs enjeux géopolitiques....22
3.5. « Code is law » : les normes techniques comme instruments de pouvoir....23
4. La spécificité des données géographiques numériques....24
4.1. La carte comme instrument de pouvoir : apports de la cartographie critique....24
4.2. La dualité ontologique des données géographiques numériques....25
5. Démarche méthodologique....26
5.1. Positionnement épistémologique et approche multiscalaire....26
5.2. Le corpus d'entretiens : diversité des acteurs et des échelles....27
5.3. L'observation participante : une immersion dans les arènes de normalisation....31
5.4. Le corpus documentaire : normes, stratégies et littérature grise....34
Conclusion de la section théorique....35
Partie 1 : Comprendre la normalisation des informations géographiques numériques....37
Chapitre I - Géopolitique et normalisation des données géographiques....38
1. La norme, à la fois outil technique et dispositif cognitif....39
1.1 Quelle Géographie pour la normalisation ?....45
1.1.1 Normalisation des données géographiques numériques et souveraineté....50
1.2 Histoire de la normalisation internationale....60

1.2.1 Le cas de la France....62
1.3 Le système français de normalisation....65
1.3.1 Le Comité de coordination et de pilotage de la normalisation (CCPN) et les comités stratégiques (co)....71
1.3.2 Les commissions de normalisation....71
1.3.3 Les bureaux de normalisation sectoriels (BN)....72
1.3.4 Le comité d'audit et d'évaluation....73
1.3.5 Le délégué interministériel aux normes (DIN)....74
1.4 L'Europe, acteur historique de la normalisation internationale....78
2. Les spécificités de l'information géographique en matière de cybersécurité et de normalisation..83
2.1. La normalisation des données géographiques....83
2.1.1 Les différentes étapes de l'adoption d'une norme internationale....86
2.2 L'intérêt des normes en matière d'information géographique....88
2.3 Cybersécurité et normalisation des données géographiques, des enjeux transverses aux domaines civil et militaire....93
3. Les enjeux du processus normatif....106
3.1 Des enjeux politiques, économiques et éthiques....106
3.2 Faut-il avoir peur de la Chine ?....112
3.3 Quelles conséquences concrètes pour l'écosystème normatif international ?....123
Conclusion du Chapitre I....128
Chapitre II- L'écosystème de la normalisation des données géographiques....129
1. Les organismes internationaux et consortiums privés au cœur de la normalisation des données géographiques....129
1.1. L'Organisation internationale de normalisation (ISO)....129
1.1.1 L'ISO/TC 211 : Informations géographiques/géomatique....133
1.1.2 La France au sein de l'ISO....137
1.1.3 Les enjeux de la gouvernance de l'ISO....142
1.2 L'Open Geospatial Consortium (OGC)....145
1.3 Le World Wide Web Consortium (W3C)....147
2. Les acteurs européens....148
2.1 Un écosystème international marqué par son interdépendance....148
2.2 La France, un poids lourd des institutions de normalisation européennes....150
2.3 Le renouveau de la stratégie européenne en matière de normalisation de données géographiques depuis les années 2000....153

3. Les acteurs de la normalisation de données géographiques militaires....162
3.1 Le Defence Geospatial Information Working Group (DGIWG)....162
3.2 l'OTAN, acteur clé de la normalisation militaire occidentale....171
3.3 Les programmes de coproduction : un outil essentiel de la production de données géographiques militaires pour l'armée française....178
Conclusion du Chapitre II....187
Chapitre III - Les enjeux de la normalisation des données géographiques....189
1. Les Enjeux des acteurs étatiques....189
1.1 Un investissement essentiel pour l'État....189
2. Le rôle des acteurs privés : entre risque et recherche d'avantage compétitif....192
3. Les enjeux de la normalisation des données géographiques pour les acteurs militaires....194
3.1 La production géographique au sein des armées....194
3.2 Les données géographiques militaires au défi de l'interopérabilité....203
3.3 La révolution GEOINT....207
Conclusion du chapitre III....216
Conclusion de la partie 1....218
Partie 2 - Risque cyber et normalisation des données géographiques....219
Chapitre IV- Les enjeux de la protection des données géographiques contre le risque cyber....220
1. Protéger les données géographiques à l'ère de la numérisation....220
1.1 Les données géographiques : des données toujours plus vulnérables aux attaques informatiques....220
1.2 : Les principes de sécurité informatique appliqués aux données géographiques : comprendre le traitement des données géographiques en ligne....222
1.3 Le rôle novateur de l'OGC en matière de cybersécurité : OGC WSS et GeoXACML....229
2. La protection des données géographiques : des enjeux en matière de responsabilité juridique et de souveraineté....233
2.1 Les différentes modalités encadrant la valeur juridique des données géographiques....234
2.2 Gouvernance et protection des données....239
2.3 Quelles évolutions concernant la souveraineté des données géographiques ?....246
3. La mise en place par de premières mesures en matière de protection de données géographiques pour les forces armées....250
3.1 Le domaine militaire et l'importance de la prise en compte du risque cyber dans la normalisation....251
3.2 Le DGIWG et la cybersécurité : comment marier sécurité et normes ouvertes ?....255

3.3 L’OTAN entre cybersécurité et interopérabilité....257
Conclusion du Chapitre IV....261
Chapitre V- Les infrastructures de données géographiques au cœur du risque cyber....264
1. Protéger les Infrastructures de données géographiques nationales, une affaire de politiques publiques....265
1.1 Les responsabilités des diffuseurs de données géographiques....266
1.2 Anticiper les risques d’attaques informatiques sur les infrastructures de données géographiques....272
1.3 Les normes : un outil clé pour développer la résilience des plateformes d’information géographique....274
2. Le CNIG, un acteur essentiel de la normalisation nationale....278
2.1 Naissance, transformations et enjeux de pouvoir institutionnels du CNIG....286
2.2 Coopérations et conflits entre acteurs nationaux : État, collectivités, agences et secteur privé 289
2.3 Les plateformes d’information géographiques en France : un paysage très hétérogène....297
3. Protéger les systèmes d’information militaires à l’heure de la cyberguerre....305
3.1 La cyberdéfense dans la doctrine française....308
3.2. Émergence du concept de guerre centrée sur les réseaux (Network Centric Warfare) et intégration de la dimension cybernétique dans la doctrine militaire américaine....318
3.3 Les normes au cœur des nouvelles infrastructures de données numériques pour les armées (Integrated Sensor Architecture)....320
Conclusion du Chapitre V....332
Chapitre VI- Les territoires au défi de la protection des données géographiques numériques....334
1. Protéger les données géographiques numériques à l’échelle infranationale....338
1.1 Les départements et les communes : acteurs importants, mais fragiles de la production de données géographiques....339
1.2 Conséquence des attaques ou pourquoi il faut améliorer la protection des collectivités....342
2. L’importance des standards de données....347
2.1 Les projets nationaux en matière de normalisation de données géographiques....348
2.2 La question de la gouvernance des données dans les échanges entre les collectivités et l’État 361
2.3 Les difficultés de l’accès aux données....365
3. Entre interconnexion, innovation et risque cyber : étude de cas du projet de jumeau numérique des territoires (JNFT)....369

3.1 Le Jumeau numérique des territoires : un programme prometteur qui fait face à de nombreux défis....377
3.2 Le Jumeau numérique des territoires au défi de la normalisation des données....382
3.3 La nécessité de la cybersécurité dans le cadre du déploiement du Jumeau numérique des territoires....386
Conclusion du chapitre VI....390
Conclusion de la partie 2....392
Partie 3 — Normalisation géospatiale et recompositions géopolitiques....395
Chapitre VII – Recomposition géopolitique et processus normatif : quel avenir pour la France et l'Europe ?....398
1. La recomposition géopolitique rebat les cartes de la standardisation internationale....399
1.1. Le renouvellement du rôle de l'Union européenne comme agent structurant des luttes de pouvoir en matière de standardisation internationale....400
1.2 L'Union européenne au défi du renouvellement de sa stratégie en matière de normalisation internationale....408
1.3 Les espaces communs de données : normaliser pour transcender les frontières européennes et exploiter au mieux les données des pays membres....418
2. Les nouvelles fractures géopolitiques dans la gouvernance des normes....427
2.1. Inégalités d'accès aux instances de normalisation pour les pays en développement....432
2.2 Vers une recomposition des alliances stratégiques régionales ?....443
2.3 Enjeux de souveraineté numérique dans les standards géographiques....450
3. L'impact des standards privés sur les normes publiques....458
3.1. Influence des grands acteurs technologiques....458
3.2. La bataille autour des formats ouverts vs propriétaires....461
3.3 Normes de facto et domination du marché au sein de l'écosystème normatif des données géospatiales....464
Conclusion du chapitre VII....467
Chapitre VIII – Le poids des nouvelles technologies dans la reconfiguration des rapports de pouvoir 468
1. L'IA et la blockchain comme nouveaux terrains de la normalisation....470
1.1. Vers une standardisation des systèmes d'intelligence géospatiale....471
1.2. Blockchain et certification de l'authenticité des données géographiques....481
1.3 Enjeux éthiques et réglementaires des nouvelles technologies....491
2. L'essor des jumeaux numériques et des métavers géographiques....504
2.1 Normalisation des infrastructures de jumeaux numériques territoriaux....504

2.2 Défis de l’interopérabilité et des réalités augmentées....506
2.3 Cybermenaces liées aux environnements immersifs....508
3. Cybersécurité post-quantique et impact sur les standards....511
3.1 Vulnérabilités des infrastructures SIG face aux technologies quantiques....513
3.2. Premiers efforts de normalisation pour la protection post-quantique....524
3.3 coopération internationale pour la sécurité quantique des données géographiques....533
Conclusion du chapitre VIII....541
Chapitre IX – Quel avenir pour la normalisation des données géographiques ?....545
1. Vers une fragmentation normative mondiale ?....547
1.1. La possibilité d’un découplage normatif à l’échelle mondiale....549
1.2 Une fracture normative internationale menacerait l’échange d’informations à l’échelle mondiale....557
1.3 Vers une guerre froide normative sans vainqueur ?....560
2. Stratégies d'influence pour les acteurs publics et privés....564
2.1. Diplomatie normative et soft power des États....564
2.2. Innovations stratégiques des consortiums privés....569
2.3. Rôle des alliances universités-industries dans l’élaboration des normes....572
3. Quel futur pour la normalisation de défense ?....577
3.1. Des défis en matière de normalisation pour l’ensemble des armées....578
3.2 La normalisation militaire au défi de la mise en réseau des armes dans tous les domaines...583
3.3 Nouvelle technologie et normalisation militaire de demain....587
Conclusion du Chapitre IX....593
Conclusion de la Partie 3....594
Conclusion générale....596
Apports de la recherche....598
Limites de la recherche....599
Perspectives de recherche....601
SOURCES PRIMAIRES....604
I.1. Entretiens semi-directifs (mars 2022 – juin 2023)....604
I.2. Observation participante (2022–2023)....604
II. Textes législatifs, réglementaires et documents institutionnels....604
II.1. Textes législatifs et réglementaires....604
III. Normes et standards....609
IV. Rapports institutionnels et documents de stratégie....612

IV.1. Documents techniques et working papers..... 617
IV.2. Ressources web institutionnelles..... 618
BIBLIOGRAPHIE..... 625
TABLE DES FIGURES ET TABLEAUX..... 659
Liste des figures..... 659
Liste des tableaux..... 661
ANNEXES — Enquête de terrain : entretiens et observations..... 662
Annexe B — Tableau récapitulatif des observations participantes..... 663
B1. Synthèse des observations par échelle..... 663
B2. Corpus d'entretiens semi-directifs (25 entretiens)..... 664
B3. Réunions observées — Échelle nationale (CNIG)..... 665
B4. Réunions observées — Échelle Défense / OTAN..... 665
B5. Réunions observées — Échelle internationale civile (ISO/TC 211)..... 667
B6. Réunions observées — Échelle internationale défense (DGIWG)..... 667
B7. Notes méthodologiques..... 668
Annexe C — Glossaire des sigles et acronymes..... 668
Annexe D — Grille d'entretien semi-directif..... 676
D1. Grille d'entretien type..... 676
Axe 1 — Parcours professionnel et positionnement institutionnel..... 676
Axe 2 — Pratiques de production et de gestion des données géographiques..... 676
Axe 3 — Relations avec l'écosystème de l'information géographique..... 676
Axe 4 — Cybersécurité et protection des données géographiques..... 677
Axe 5 — Souveraineté numérique et enjeux géopolitiques..... 677
D2. Adaptations selon les profils d'acteurs..... 679
Acteurs de la défense (DGA, BGHOM, 28e Groupe géographique)..... 679
Acteurs territoriaux (DREAL, DEAL, Régions, CRIGE)..... 679
Experts normalisation (IGN, AFNOR, délégués ISO/TC 211)..... 679
Acteurs de la cybersécurité (ANSSI)..... 679
D3. Conditions de réalisation des entretiens..... 679
Annexe E — Cartographie de l'écosystème normatif géospatial..... 681
F1. Acteurs de la normalisation géospatiale par niveau..... 681
E2. Principales relations entre acteurs..... 684
E3. Architecture multiniveau de la normalisation..... 684
E4. Position de la France dans l'écosystème..... 685

Annexe F — Tableau des principales normes géospatiales 686
Normes ISO (série 19100 — Information géographique) 686
Standards OGC (Open Geospatial Consortium) 687
Standards de défense (DGIWG, OTAN) 688
Standards hydrographiques (OHI / IHO) 688
Standards nationaux (CNIG France) 689