université PARIS-SACLAY

NNT : 2018SACLS023

Thèse de doctorat

UNIVERSITÉ PARIS SUD
Comprendre le monde, construire l'avenir

UNIVERSIDAD PANAMERICANA

L'usurpation d'identité numérique sur Internet : Etude comparée des solutions françaises, mexicaine et nord-américaines

Thèse de doctorat de l'Université Paris-Saclay
Préparée à la Faculté Jean Monnet de l'Université Paris Sud

École doctorale SHS n°578 Sciences humaines et sociales,
Spécialité de doctorat : Droit Privé et Sciences Criminelles.
Laboratoire de recherche : Centre d'Études et de Recherche en Droit de l'Immatériel

Thèse présentée et soutenue à Ville de Sceaux, le 22 janvier 2018, par

Cynthia Gabriela Solís Arredondo

Composition du Jury :

Alexandra BENSAMOUN Professeur, Université de Rennes 1	Président
Alexandra BENSAMOUN Professeur, Université de Rennes 1	Rapporteur
Javier PUYOL Professeur, Universidad Internacional de La Rioja	Rapporteur
Vincent LEMOINE Expert judiciaire – Docteur en Droit	Examinateur
Antoine LATREILLE Doyen, Faculté Jean Monnet, Université Paris Sud	Directeur de thèse
Alfredo REYES KRAFFT Docteur, Université Panaméricaine	Co-Directeur de thèse

Titre : L'usurpation d'identité numérique sur Internet : Etude comparée des solutions françaises, mexicaine et nord-américaines.

Mots clés : Usurpation d'identité, données personnelles, cybercriminalité

Résumé : La présente étude se concentre sur le concept d'identité, une partie fondamentale de la personne ; compris non seulement comme une entité biologique et naturelle, mais comme une entité sociale, dotée de divers éléments qui constituent sa personnalité. C'est pourquoi l'importance de sa protection est mise en évidence, on ne peut pas quantifier la valeur de quelque chose jusqu'à ce qu'on comprenne l'importance qu'elle a pour son propriétaire. Le concept d'identité décrit dans ce schéma de droit comparé est celui de la personne physique.
Même lorsqu'il s'agit d'une liste d'informations personnelles, selon certains facteurs inhérents à la personne ; tels que sa position, sa notoriété, sa position sociale ; la divulgation de ces données représente une certaine valeur. L'identité dans les réseaux sociaux, dans la société de nos jours, est devenue plus importante.
L'entité « social 2.0» a parfois une valeur supérieure à celle de son propre rôle dans la société. Comme le mentionnent les auteurs Nicholas Christakis et James Fowler, dans leur livre "Connected", les réseaux sociaux sont une sorte de « superorganisme » humain. Ils ont une vie propre. Ils peuvent grandir et évoluer. Par conséquent, l'étude du phénomène des réseaux sociaux sur Internet et de notre interaction dans ce monde virtuel mérite une attention particulière et une étude approfondie. Ils font maintenant partie de notre vie, de notre quotidien, nous créons des relations affectives et générons un sentiment d'appartenance et de communauté. Etonnamment, nous continuons à obéir au même principe social, à nous chercher nous-mêmes à travers de ceux à qui on ressemble.

Title : Digital identity theft on the Internet: Comparative study of French, Mexican and North American solutions.

Keywords : Cybercrime, Identity theft, privacy

This study focuses on the concept of identity, a fundamental part of the person; understood not only as a biological and natural entity, but as a social entity, endowed with various elements that constitute its personality. That's why the importance of its protection is highlighted, we can not quantify the value of something until we understand the importance it has for its owner. The concept of identity described in this scheme of comparative law is that of the natural person. Even when it is a list of personal information, according to certain factors inherent to the person; such as his position, his reputation, his social position; the disclosure of these data represents a certain value. Identity in social networks, in today's society, has become more important.
The "social 2.0" entity sometimes has a value greater than that of its own role in society. As noted by authors Nicholas Christakis and James Fowler, in their book "Connected", social networks are a kind of human "superorganism". They have a life of their own. They can grow and evolve. Therefore, the study of the phenomenon of social networks on the Internet and our interaction in this virtual world deserves special attention and a thorough study. They are now part of our life, our daily lives, we create affective relationships and generate a sense of belonging and community. Surprisingly, we continue to obey the same social principle, to seek ourselves through those to whom we resemble.

ÍNDICE

USURPACIÓN DE IDENTIDAD DIGITAL: UN ESTUDIO COMPARATIVO DE LAS SOLUCIONES FRANCESAS, MEXICANAS Y NORTEAMERICANAS.

J'avais envie d'adresser mes sincères remerciements à ceux qui ont contribué à la réalisation de ce rêve. Je tiens tout particulièrement à remercier à Monsieur Antoine Latreille, de croire en moi depuis 2006

Á Monsieur Alfredo Reyes Krafft, qui m'a soutenu, encouragé, et avec qui j'ai établi une relation de confiance et de solidarité en tout moment, merci d'avoir accepté diriger ma thèse dès le premier jour

Á mes amis qui ont toujours resté avec moi, même à la distance, même depuis autres places dans l'Univers, Éléo, Patrick, Viviana, Juan Carlos, Cédric†, Elia† et Rabeb†

Á ma mère

Aux chers membres du jury, Alexandra Bensamoun, Javier Puyol et Vincent Lemoine, pour votre précieux temps, compréhension et patience.

A mes frères mexicains mortes le 19 septembre 2017, et les héros qui se sont battu pour sauver les vies des autres.

SIGLAS Y ABREVIATURAS

AFORE	Administradoras de Fondos para el Retiro
AICPA	American Institute of Chartered Public Accountants
AMIPCI	Asociación Mexicana de Internet ahora Asociación de Internet MX
APEC	Foro de Cooperación Económica Asia-Pacífico
Art.	Artículo
CC	Código Civil
CCo	Código de Comercio
CIA	Central Intelligence Agency
CICA	Canadian Institute of Chartered Accountant
CNBV	Comisión Nacional Bancaria y de Valores
CNIL	Comisión Nacional de Informática y Libertades
CONDUSEF	Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros
COPPA	Children's Online Privacy Protection Act
CPEUM	Constitución Política de los Estados Unidos Mexicanos
CPF	Código Penal Federal
CURP	Clave Única del Registro de Población
DMCA	Digital Millenium Copyright Act
EC3	European Cybercrime Centre
ECPA	Electronic Communications Privacy Act
EEUU	Estados Unidos de América
ETC	Etcétera
EUROPOL	Oficina Europea de Policía
FBI	Federal Bureau of Investigation
FCA	Federal Communciations Act
FEA	Firma Electrónica Avanzada
FISA	Foreign Intelligence Surveillance Act
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
IFAI	Instituto Federal de Acceso a la Información y Protección de Datos
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
INE	Instituto Nacional Electoral
INTERPOL	Organización Internacional de Policía Criminal
ITADA	Identity Theft and Assumption Deterrence Act
ITU	International Telecommunication Union
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LIL	Ley de informática y Libertades
NIR	Numéro d'Inscription au Répertoire des Personnes Physiques
OAS	Organization of American States
OCDE	Organización para la Cooperación y el Desarrollo Económicos
PCLOB	Privacy and Civil Liberties Oversight Board
PROFECO	Procuraduría Federal del Consumidor
PS	Privacy Shield
RFC	Registro Federal de Contribuyentes

RLFPDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
SAR	Sistema de Ahorro para el Retiro
SAT	Servicio de Administración Tributaria
SH	Safe Harbor
TIC	Tecnologías de la Información y la Comunicación
TLCAN	Tratado de Libre Comercio de América del Norte
UE	Unión Europea

INTRODUCTION GENERALE

L'identité numérique des personnes est devenue un des plus importantes valeurs immatérielles dans la vie quotidienne, la réputation personnel, académique, le profil et le déroulement de la carrière professionnelle, mais encore plus que ça, la liberté d'être sur la toile sans avoir peur de l'usurpation de notre identité est l'inspiration de ce travail de thèse.

Dans le monde numérique les frontières n'existent plus, les interactions avec les personnes de tout le monde sont de plus en plus courantes, le commerce électronique, les réseaux sociaux, les démarches administratives en ligne, l'échange d'information entre pays et gouvernements, et aussi les rapports romantiques dans les applications mobiles, c'est aussi la raison d'être une étude de droit comparé entre le droit mexicain, français et américain.

Dans la première partie nous développons les éléments de l'identité numérique, les données personnelles comprises dans l'ensemble de ce concept qui est à la fois mal compris et en conséquence mal protégé mais aussi très importante dans le développement de l'économie numérique.

La deuxième partie, comprends les interprétations de l'identité numérique dans le domaine du droit pénal du droit administratif et du droit civil et commercial.

Il y a notamment des différences entre l'interprétation qui fait le droit pénal de l'identité en tant que bien juridique protégé ; en comparaison avec les interprétations du droit administratif qui protège l'identité numérique en tant que donnée personnelle, la mise en œuvre de la reconnaissance international du droit à la protection des données à caractère personnel et devient la régulation qui définit les règles du leur traitement, ainsi qui impose les sanctions au traitement illicite et de l'autre côté le droit civil qui d'une parte reconnait le droit de la personnalité et le droit à l'image.

La troisième partie est dédiée à l'étude de l'identité numérique comme source d'évolution du droit, ainsi qu'aux atteintes à l'ensemble des éléments qui font partie de cette identité. Le droit est toujours derrière l'innovation et malgré tout, à côté de l'évolution de l'humanité, des inventions, de la technologie et du développement, il existe l'évolution des actes illicites et de moyens de commission des délits dans l'endroit numérique.

Même si le phénomène de l'usurpation d'identité n'est pas nouveau, il a surmonté dans le monde dans les cinq derniers années grâce aux nouvelles technologies qui permettent de créer, modifier, altérer, falsifier, reproduire et diffuser donnés personnelles, photos et identifiants de façon très rapide et au niveau mondial, ce qui permet de vendre dans le marché noir plein des données personnelles pour après faire diffèrent types d'utilisation illicite, notamment l'usurpation d'identité.

Ainsi comme la nouvelle technologie sert à la sophistication des activités illicites, il existe un travail des entreprises de sécurité informatique pour lutter de façon technique contre les atteintes aux systèmes d'information, aux réseaux et à l'information, en particulier les atteintes aux données personnelles, donc, à la fin de cette partie on fait une étude des outils numériques crées à cet effet.

Trouver notre place dans le monde devrait être la mission première de la vie. S'identifier, se séparer de tout ce qui ne nous appartient pas, et une fois que nous connaissons les éléments qui nous composent, notre précieuse identité, nous pouvons nous considérer comme des entités utiles pour la société, digne dans notre propre essence et digne de nos actes.

La présente étude se concentre sur le concept d'identité, une partie fondamentale de la personne ; compris non seulement comme une entité biologique et naturelle, mais comme une entité sociale, dotée de divers éléments qui constituent sa personnalité. C'est pourquoi l'importance de sa protection est mise en évidence, on ne peut pas quantifier la valeur de quelque chose jusqu'à ce qu'on comprenne l'importance qu'elle a pour son propriétaire. Le concept d'identité décrit dans ce schéma de droit comparé est celui de la personne physique.

Même lorsqu'il s'agit d´une liste d'informations personnelles, selon certains facteurs inhérents à la personne ; tels que sa position, sa notoriété, sa position sociale ; la divulgation de ces données représente une certaine valeur, qui ne serait pas la même pour le président des États-Unis d'Amérique que pour un citoyen ordinaire du même pays. Par exemple, on se rappellera du cas de l'ancien président Bill Clinton en matière de divulgation d´ affaires extra-conjugales, lorsqu´ une série d'enregistrements au contenu explicite a été publiée.

Par conséquent, nous prétendons, dans une large mesure, que l'individu soit capable d´ « évaluer » son identité en fonction des éléments particuliers qui le composent, et soit conscient des risques inhérents à la divulgation de certaines informations pour qu´il les gère de manière équilibrée.

Par exemple en France, pays qui constitue l'étude de droit comparé que je présente, diverses opinions d'auteurs reconnus ont conclu que l'important n'est pas que l'individu n'ait pas de présence sur Internet, mais au contraire, qu'il ait une présence correctement gérée, qu´il décide

de manière consciente le type d'information qu'il divulgue et à quelles fins. L'auteur Daniel Kaplan dit: « La valeur de la vie privée, c'est de nous permettre d'avoir une vie publique », dans son livre « Informatique, libertés, identités ».

L'intention de cette analyse du phénomène criminel d '"Usurpation ou vol d'identité", est de faire connaitre les facteurs de risque et d'anticiper leurs dommages, ou au moins, de diminuer leurs conséquences.

Je considère ce chapitre d'une importance fondamentale, car il ne définit pas seulement l'identité - le sujet de mon étude - mais aussi la particularité de l'identité des individus et leur présence dans les réseaux sociaux sur Internet.

L'identité dans les réseaux sociaux, dans la société de nos jours, est devenue plus importante. L'entité « social 2.0» a parfois une valeur supérieure à celle de son propre rôle dans la société. Comme le mentionnent les auteurs Nicholas Christakis et James Fowler, dans leur livre "Connected", les réseaux sociaux sont une sorte de « superorganisme » humain. Ils ont une vie propre. Ils peuvent grandir et évoluer. Par conséquent, l'étude du phénomène des réseaux sociaux sur Internet et de notre interaction dans ce monde virtuel mérite une attention particulière et une étude approfondie. Ils font maintenant partie de notre vie, de notre quotidien, nous créons des relations affectives et générons un sentiment d'appartenance et de communauté. Etonnamment, nous continuons à obéir au même principe social, à nous chercher nous-mêmes à travers de ceux à qui on ressemble.

En fin, le travail présent, a pour objet développer le phénomène de l'usurpation d'identité à l'égard de la loi des trois pays ainsi que les instruments en vigueur pour lutter contre le traitement illicite des données personnelles qui conforment l'identité numérique.

Université Paris-Saclay
Faculté Jean Monet, Université Paris Sud
54, Boulevard Desgranges
92330 SCEAUX

Llevar a cabo una investigación de derecho comparado, implica la obligación moral, de conocer la historia y condiciones sociopolíticas y económicas, así como de conocer la tradición jurídica de cada uno de los países en estudio, toda vez que el aparato legislativo de cada uno, obedece a realidades y necesidades que pueden parecer muy distintas pero que presentan interesantes puntos de contacto, muchas veces desconocidos.

La problemática de la usurpación de identidad, es multidimensional, internacional y añeja; de la misma manera, la identidad es un concepto a geometría variable y complejo, compuesto de elementos de hecho y de derecho, de anatomía, psicología, sociología y desde un punto de vista filosófico, también de teología; y ahora, de tecnología.

A lo largo de este trabajo de tesis, desarrollaremos el concepto de identidad digital, una de las tantas caras del caleidoscopio de la identidad humana, hoy en día, la más frecuente y por ende, la más susceptible a la delincuencia.

Tras dimensionar la importancia del concepto de identidad digital, nos implicamos en la materia que nos apasiona y nos ocupa, que es la forma en que las legislaciones de los tres países que comprenden este estudio, reconocen, regulan y garantizan el derecho humano a la identidad y particularmente, conocer los esfuerzos independientes y en conjunto, por extender este esquema de protección a la identidad digital, en los casos que así se requiera.

La idea central de este trabajo es el estudio de las leyes y tratados internacionales existentes en los tres países para establecer una estrategia legal de protección y defensa en el presente, sin necesidad de siempre recurrir al interminable y a veces infértil, proceso legislativo.

La velocidad con la que hoy en día interactúan los seres humanos, gracias al uso de su identidad digital, obliga a los juristas y autoridades de todo el mundo, a proponer soluciones creativas, con elementos existentes.

Es cierto, el derecho es materia viva y obedece a las necesidades humanas, sin embargo, en la mayoría de los casos, no hay problema jurídico, que no pueda resolverse gracias a la correcta aplicación de los principios generales del derecho, las bases del derecho civil e incluso del derecho romano; por lo que en múltiples ocasiones durante la lectura de esta obra, se cuestiona la auténtica necesidad de crear nuevas leyes adaptadas al mundo digital, o bien, simplemente saber utilizar los aparatos legales existentes.

Como parte de la evidencia que nos permite constatar que la usurpación de identidad digital es un problema creciente, en la tercera parte presentamos los casos más trascendentes de usurpación de identidad, los casos que se visualizan como una tendencia para los próximos años y las cifras económicas de los daños causados hasta el momento por ilícitos cometidos en contra de la identidad digital, en los tres países que forman parte del presente estudio.

¿Qué tan importante puede ser para nosotros nuestra identidad[1] digital? Desgraciadamente, no podemos estimar, cuantificar, ni medir el impacto que causaría en nuestras vidas, en caso de que fuera usurpada[2]...hasta que nos sucede y comenzamos a sufrir las consecuencias de este acto delictivo.

Las empresas más importantes de seguridad informática se han dado a la tarea no sólo de investigar acerca del aumento en la incidencia de este tipo de vulneraciones de seguridad, sino de cuantificar el impacto social y económico de los mismos, por sí mismas o a través de asociaciones sin fines de lucro como el Identity Theft Resource Center[3]; los reportes más recientes de dicha institución, indican que, sumado a otros ataques informáticos, la usurpación de identidad, de permanecer impune en la mayoría de los casos, podría llevarnos a una situación de caos mundial y a la necesidad de implementar medidas de autenticación cada vez más complejas y sofisticadas, que incluso, pondrían en situación de vulnerabilidad la esfera más íntima del individuo, pues estos instrumentos biométricos también son falibles y falsificables aun cuando esto último represente un mayor grado de dificultad para los delincuentes.

El punto central de esta investigación doctoral es la comprobación de las consecuencias jurídicas, psicológicas, sociales y económicas que podría ocasionar en un futuro inmediato el delito de usurpación de identidad, a través de estudios[4] realizados por empresas de seguridad informática[5] y gobiernos de distintos países; a su vez, también se analizan los instrumentos jurídicos vigentes en los tres países citados, para comprobar su eficacia en la prevención y combate a esta actividad

[1] Identidad 2.0, Wikipedia, en: http://es.wikipedia.org/wiki/Identidad_2.0 consultado el 20 de noviembre de 2013.

[2] Usurpar; Diccionario de la lengua española (DRAE). La edición actual ―la 22.a, publicada en 2001. En; http://lema.rae.es/drae/?val=usurpar consultado el 20 de noviembre de 2013.

[3] *Identity Theft Resource Center 2013 Data Breach Stats* http://www.idtheftcenter.org/images/breach/ ITRC_Breach_Stats_Report_2013.pdf consultado el 28 de noviembre de 2013.

[4] *Internet Security Threat Report. Symantec 2013*. En: http://www.symantec.com/content/en/us/enterprise/ other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf consultado el 28 de noviembre de 2013.

[5] Informe sobre las amenazas para la seguridad en Internet de 2017. En https://www.symantec.com/es/mx/ security-center/threat-report, consultado el 9 de diciembre de 2017.

delictiva que pone en riesgo nuestra identidad, como fruto de un mal uso y gestión de nuestros datos personales así como de elementos propios de nuestra personalidad.

El objetivo final, luego de un análisis minucioso de dichos instrumentos jurídicos vigentes; es evidenciar los efectos nocivos del robo[6] de identidad digital para los ciudadanos de en estos países y su impacto en la economía de los mismos, y quizás, en algún momento muy cercano, lograr que sea catalogado como delito federal en México, atendiendo la gravedad de sus consecuencias, tanto en la reputación, el honor y e incluso los riesgos para la vida misma de la víctima.

[6] En Estados Unidos, el nombre del delito que analizamos es Identity Theft and Identity Fraud, según la traducción obtenida del Diccionario Oxford, el término correcto es robo, en: http://www.oxforddictionaries.com/ es/traducir/ingles-espanol/theft consultado el 25 de noviembre de 2013. Para fines prácticos, utilizaremos robo de identidad al referirnos a la legislación estadounidense.

PRIMERA PARTE

LA IDENTIDAD DIGITAL. UN RETO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

Encontrar nuestro lugar en el mundo, debería ser la misión primaria de la vida, individuarnos, separarnos de todo aquello que no nos pertenece, y una vez conociendo los elementos que nos conforman, nuestra valiosa identidad, podemos concebirnos como entes útiles para la sociedad, dignos en nuestra propia esencia y dignos nuestros actos por añadidura.

El presente estudio, se centra en el concepto de identidad, pieza fundamental de la persona; comprendida no sólo como un ente biológico y natural, sino como un ente social, dotado de diversos elementos que constituyen su personalidad. De ahí que se destaque la importancia de su protección, no podemos cuantificar el valor, incluso monetario, de cualquier cosa, sino hasta que comprendemos la importancia que tiene para su titular. El concepto de identidad que se describe en este esquema de derecho comparado, es el de la persona física.

Incluso tratándose del mismo listado de información personal, dependiendo de ciertos factores inherentes a la persona, como su cargo, fama, posición social; la divulgación de ésta cobra un peso específico, no tendrá el mismo valor para el presidente de los Estados Unidos de América, que para un ciudadano común y corriente del mismo país, el hecho de que se difundiera información relativa a relaciones extramaritales; como recientemente ha sucedido con el ex presidente Bill Clinton[7], al difundirse una serie de grabaciones con contenido explícito.

Por tanto, parte de nuestra pretensión es, en gran medida, que el individuo logre "valuar"[8] su identidad en función de los elementos particulares que la componen, y tome conciencia de los riesgos que conlleva la divulgación de cierta información y gestione de forma equilibrada la misma.

Por ejemplo, en Francia, país que compone el estudio de Derecho comparado que presento, diversas posturas de reconocidos autores han concluido que lo importante no es que el individuo no tenga presencia en Internet, sino por el contrario, que tenga una presencia correctamente gestionada,

---

[7] Hirania Luzardo The Huffington Post. *Clinton-Lewinsky: Sale a la luz grabación con "contenido sexual"* En: http://voces.huffingtonpost.com/2013/08/02/monica-lewinsky-tape-sex_n_3695977.html consultado el 20 de noviembre de 2013.

[8] *Valuar; Diccionario de la lengua española (DRAE). La edición actual ―la 22.a, publicada en 2001*. En: http://lema.rae.es/drae/?val=valuar consultado el 20 de noviembre de 2013.

que cuente con un juicio correcto del tipo de información que divulga y para qué fines. Ya lo dice el autor Daniel Kaplan[9], "El valor de la vida privada, consiste en permitirnos tener una vida pública", en su libro "Informática, libertades identidades".

La intención de este análisis del fenómeno delictivo de "Usurpación o robo de identidad", es dar a conocer los factores de riesgo y prevenir su comisión, o en su defecto disminuir su incidencia.

Este capítulo lo considero de fundamental importancia, ya que no sólo define la identidad -materia de mi estudio-, sino la particularidad de la identidad de los individuos y su presencia en redes sociales en Internet.

La identidad en redes sociales, bajo la óptica actual de la sociedad, ha cobrado mayor relevancia; el "ente social 2.0" en ocasiones tiene un valor mayor que el de su propio rol en la sociedad. Tal y como lo mencionan los autores Nicholas Christakis y James Fowler, en su libro "Conectados" [10]; las redes sociales son una especie de "superorganismo" humano. Tienen vida propia. Pueden crecer y evolucionar. Por lo tanto, el estudio del fenómeno de las redes sociales en Internet y nuestra interacción en ese mundo virtual, merece una especial atención y profundo estudio; ahora son parte de nuestra vida, de nuestro día a día, creamos relaciones afectivas y sentimiento de pertenencia y comunidad; y, sorprendentemente, seguimos obedeciendo a un mismo principio social, buscarnos en aquellos en los que encontramos semejanzas.

[9] KAPLAN, Daniel, *Informatique, libertés, identités*, FYP éditions, France, 2010.
[10] CHRISTAKIS, N.A. y FOWLER J.H., *Conectados, el sorprendente poder de las redes sociales y cómo nos afectan*, Taurus, México, 2013, p.14.

CAPÍTULO I

EL CONCEPTO DE IDENTIDAD DIGITAL

1.1 CONCEPTO HOLÍSTICO DE IDENTIDAD

A lo largo de la historia, la identidad, obedece a una tendencia; identificar en todos los casos, significa singularizar.

En la Edad Media, la identidad debía ser legible y visible, por ello, existía un vínculo estrecho entre la identidad y la vestimenta, para poder de alguna manera clasificar a los habitantes y así otorgarle el tratamiento debido, ya sea en cuanto a las prerrogativas o a sus restricciones, dependiendo de su rol en la sociedad[11].

La identificación escrita, se impone a partir del siglo XIV; siempre a la medida en que la autoridad requirió delimitar la identidad individual.

La sistematización de la identificación responde sucesivamente a la necesidad estadística que impone un conocimiento preciso de la población, a la conformación y movilización del ejército y al diseño de planes de desarrollo social[12].

Hoy en día, se ha generado una creciente ambición por describir al individuo a tal detalle que se incluyan sus características físicas y signos particulares para su identificación precisa; con la ayuda de algunas ciencias auxiliares, tales como, la antropometría y la biometría hoy en día puede identificarse a un individuo de forma casi infalible.

El concepto de individuo suele tener diferentes significados, tanto biológicos, como sociológicos y antropológicos, por ejemplo: el que utilizaré a lo largo de este estudio que es el definido por la Real Academia Española, en su sentido coloquial "Persona, con abstracción de las demás". Justamente porque la idea de identidad que quiero explorar es aquella que nos brinda elementos de separación de los demás, del vulgo, que nos saca del anonimato, nos vuelve especiales y únicos en función de la pertenencia a una sociedad.

[11] FOREST, David, *Droit des données personelles*, Gualino éditeur, Lextenso éditions, París, 2011, p.15.
[12] *Ibidem.*

A este conjunto de características propias de un individuo en relación con el cúmulo de individuos que lo rodean, se le denomina identidad.

Del latín identitas, la identidad es el conjunto de los rasgos propios de un individuo o de una comunidad. Estos rasgos caracterizan al sujeto o a la colectividad frente a los demás.

La identidad también es la conciencia que una persona tiene respecto de sí misma y que la convierte en alguien distinto a los demás. Aunque muchos de los rasgos que forman la identidad son hereditarios o innatos, el entorno ejerce una gran influencia en la conformación de la especificidad de cada sujeto.

Del Diccionario de la Real Academia de la Lengua Española, podemos extraer la siguiente definición:

> *identidad*[13].
>
> *(Del b. lat. identĭtas, -ātis).*
>
> *1. f. Cualidad de idéntico.*
>
> *2. f. Conjunto de rasgos propios de un individuo*[14] *o de una colectividad que los caracterizan frente a los demás.*
>
> *3. f. Conciencia que una persona tiene de ser ella misma y distinta a las demás.*
>
> *4. f. Hecho de ser alguien o algo el mismo que se supone o se busca.*
>
> *5. f. Mat. Igualdad algebraica que se verifica siempre, cualquiera que sea el valor de sus variables.*

[13] *Identidad; Diccionario de la lengua española (DRAE.)* La edición actual — la 23.a, publicada en 2014. http://dle.rae.es/?id=KtmKMfe. Consultado el 20 de diciembre de 2017.

[14] *Individuo; Diccionario de la lengua española (DRAE). La edición 22.a, publicada en 2001*. En: http://lema.rae.es/drae/?val=individuo . Consultado el 20 de noviembre de 2013.

Analizando las diversas acepciones de la definición propuesta, podemos decir lo siguiente:

1. La cualidad de idéntico, nos habla de que al comparar algo con su símil, resulta ser igual, es decir, nos habla de las características propias de un algo o alguien que coinciden con otro de su misma clase o especie.

2. Al hablar de los individuos o de las colectividades, nos encontramos con la necesidad de encontrar sus rasgos propios que los diferencian de los demás.

3. El individuo a lo largo de su vida, encuentra rasgos propios en su ser, para distinguirse de los demás; la búsqueda de la identidad propia, en efecto, se convierte en muchos casos en una lucha continua y necesaria, toda vez que no existiría individuo, si no fuera posible discriminarlo de los demás.

4. El uso de la palabra "identidad" en el lenguaje de los investigadores, se da cuando hay un algo o alguien de quien debe acreditarse su personalidad o su ser.

5. Incluso en el lenguaje de las matemáticas, de nuevo retomamos los conceptos de comparación y de igualdad.

1.2 LA IDENTIDAD COMO FIN PRIMARIO DEL INDIVIDUO.

Como hemos mencionado antes, la identidad debe ser comprendida más allá de un mero contexto semántico, luego entonces, se convierte en un fin en sí misma, la comprensión del individuo como ente único, valioso, digno y elemento primordial de la sociedad, es lo que da, en gran medida, sentido a la vida del mismo. Por lo tanto, el fin primario del ser humano debiese ser el encontrar su lugar en el mundo, visualizarse y asumirse en su totalidad como un ser compuesto de elementos tangibles e intangibles, tales como aquellos correspondientes a su estructura más básica, es decir, su anatomía; pero también aquellos elementos de carácter filosófico, psicológico, y en general, de su personalidad, que, en su conjunto, integran a lo que conocemos como individuo.

Carl Jung, miembro de la corriente de la psicología analítica, postulaba que el propósito supremo de la vida es la individuación, las experiencias de la niñez en suma con las de la madurez y las esperanzas del futuro hacen al individuo ser lo que es; de hecho, sobre él mismo, decía "Mi vida es un caso de la autorrealización del inconsciente. Todo lo que hay en él busca su manifestación externa, y la personalidad también dese evolucionar para salir de sus estados inconscientes"[15].

Para él, la individuación, es un estado de salud psicológica que se deriva de la integración de todos los aspectos conscientes e inconscientes de la personalidad. En pocas palabras, la individuación implica convertirse en un individuo, en realizar las capacidades propias y en desarrollar el sí mismo. La tendencia a la individualización es innata e inevitable, pero las fuerzas ambientales, como las oportunidades económicas y educativas y la índole de la relación progenitor e hijo, la impulsan o la obstaculizan.

Para lograr la individuación, las personas deben abandonar las conductas y los valores que digirieron en la primera mitad de la vida y encarar el inconsciente, llevándolo a la consciencia y aceptando lo que les pide que hagan. Deben escuchar lo que dicen sus sueños y seguir sus fantasías, ejercitando la imaginación creativa escribiendo, pintando o mediante otro tipo de expresión. Sólo así se revelará el sí mismo[16].

[15] SCHULTZ D.P. y SCHULTZ S.E., *Teorías de la Personalidad*, 9a ed. Cengage Learning, México, 2013, 99-127.
[16] *Ibidem.*

Desde luego que no promovía el dejarse dominar por el inconsciente, sino equilibrarlo con la fuerza consciente para ser un individuo emocionalmente maduro; a lo que yo, personalmente, llamaría el conocerse y gobernarse.

Más adelante, esta teoría apoyará la hipótesis en la que sostengo que muchos sujetos que han reprimido sus más primarios instintos y tienen una personalidad introvertida, suelen dejar salir ese cúmulo de elementos de personalidad real a través de sus "avatares" o personajes en redes sociales.

Al respecto, Jean-Claude Filloux, en su libro La personalidad; postula que la psicología tiene como fin esencial: el conocimiento del individuo como ente particular "jamás nos encontramos ante el hombre en general, sino siempre ante un hombre particular, un individuo que con frecuencia es un enigma, un problema y bien sabemos que la solución no puede encontrarse sino en él mismo. La característica más esencial del hombre es su individualidad"[17].

Filloux destaca un elemento que coincide a la perfección con mi postura respecto al tema y es, que el hombre a través de su individualidad se manifiesta y comporta como ningún otro, ya que dicho comportamiento pertenece tan sólo a él; si bien es cierto que el hombre es un ente social y como tal, se encuentra impregnado de las influencias que ejerce la sociedad en su vida, siempre conserva elementos propios que servirán para distinguirlo como ente particular y único.

Fundamento mi anterior postura, coincidiendo con lo que, respecto de la dignidad del hombre, argumenta el Doctor Carlos Llano Cifuentes en su obra "Viaje al centro del hombre"; el ser humano por el simple hecho de existir, es un ente dotado de dignidad, de valor en sí mismo, un valor que logra dotar a todos los hechos que de él emanan, de valor. Sus actos son valiosos en la medida de su origen, es decir, que provienen del ser humano, y, por tanto, de un ser digno. "Cada individuo, cada uno de nosotros, aunque se sepa limitado por su nacimiento y su muerte y por todas aquellas circunstancias que lo constriñen y empobrecen, tiene valor infinito"[18]. Pero, sin duda alguna, la esencia del pensamiento del autor que quiero enfatizar como fundamento de mi postura respecto del valor de

[17] FILLOUX, Jean Claude, *La personalidad*, Presses Universitaires de France, Trad, Publicaciones Cruz O. S.A., México 1992, p.3.
[18] LLANO CIFUENTES, Carlos, *Viaje al Centro del hombre*, Ediciones Rialp, Madrid, 2010

cada uno de nosotros como individuos, es que las personas no son intercambiables por ser en sí mismas un universo completo.

1.3 LA IDENTIDAD COMO BIEN JURÍDICO

El derecho a la identidad es uno de los derechos fundamentales de todo ser humano, y es necesario para poder beneficiarse de los otros derechos fundamentales.

Desde que nacemos, contamos con derechos propios de identidad, por ejemplo, el derecho a tener un nombre y un apellido, la organización internacional sin fines de lucro, Humanium, señala los siguientes derechos del niño en relación a la identidad:

> *"El derecho del niño a la identidad: Desde el momento de su nacimiento, toda persona tiene derecho a obtener una identidad. La identidad incluye el nombre, el apellido, la fecha de nacimiento, el sexo y la nacionalidad. Es la prueba de la existencia de una persona como parte de una sociedad, como individuo que forma parte de un todo; es lo que la caracteriza y la diferencia de las demás.*
>
> *Todos los niños tienen derecho a poseer una identidad oficial, es decir, a tener un nombre, un apellido, una nacionalidad y a conocer la identidad de sus progenitores.*
>
> *Derecho a un nombre y un apellido: Desde su nacimiento, el niño tiene derecho a tener un nombre y un apellido. Todo niño debe ser registrado inmediatamente después de su nacimiento, ya que los padres tienen la obligación de informar el nombre, el apellido y la fecha de nacimiento del recién nacido.*
>
> *Esta acción supone el reconocimiento inmediato por parte del Estado de la existencia del niño, y la formalización de su nacimiento ante la ley. Además, su registro permitirá al niño preservar sus orígenes, es decir, las relaciones de parentesco que lo unen a sus padres biológicos.*

Derecho a la nacionalidad: Desde su nacimiento, un niño tiene derecho a adquirir una nacionalidad."[19]

Los atributos de la personalidad, en Derecho, son aquellas propiedades o características de identidad propias de las personas físicas o jurídicas en tanto que titulares de derechos.[20]

Jeremy Antippas, graduado de la Universidad Panthéon-Assas, explica en su tesis doctoral, respecto de los derechos de la personalidad, que "pueden estar definidos como los derechos que aseguran al individuo la reserva de los atributos de su persona, ya sea garantizando su integridad moral: como el derecho al secreto de la vida privada, derecho a la imagen, sobre la voz y el apellido, derecho al respeto del honor y la presunción de inocencia y de la dignidad de la persona humana, en fin, derecho moral, por los autores, artistas, intérpretes de obras intelectuales que constituyen la expresión de su personalidad. La teoría general de los derechos de la personalidad en Francia, son fruto de un trabajo arduo de la doctrina privatista y de la jurisprudencia desde hace aproximadamente un siglo. Ella se completa a través del estudio de una multiplicidad de áreas del derecho, no sólo el civil sino el penal, de la propiedad intelectual, etc."[21]

Cabe destacar, el énfasis que hace en el postulado de que los derechos de la personalidad nacen tradicionalmente de la doctrina del derecho civil, poco a poco han ido migrando hacia el derecho administrativo; ciertamente, en México sucede exactamente lo mismo, si tomamos en cuenta que la autoridad garante de la protección de los datos personales de los ciudadanos mexicanos, el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), recientemente convertido en organismo autónomo cambiando de nombre a INAI[22] , es de índole administrativa, tal como lo es la autoridad homóloga en Francia, la Comisión Nacional de Informática y Libertades (CNIL).

---

[19] *Humanium, Derecho a la identidad* en: http://www.humanium.org/es/derecho-identidad/ Consultado el 30 de agosto de 2013.

[20] Atributos de la personalidad, W ikipedia, en: http://es.wikipedia.org/wiki/ A tributo_de_la_personalidad consultado el 17 de julio de 2013.

[21] Jeremy Antippas, *Les droits de la personnalité : de l'extension au droit administratif d'une théorie fondamentale de droit privé*, publicada el 25 de octubre de 2011. En: http://www.u-paris2.fr/29472577/0/fiche___article/ consultado el 25 de noviembre de 2013.

[22] INAI, Organismo autónomo, comunicado oficial. http://inicio.ifai.org.mx/Comunicados/ Comunicado%20IFAI-001-14.pdf. Consultado el 30 de abril de 2014.

Los llamados derechos de la personalidad forman parte de lo que se conoce como el patrimonio moral, la noción de patrimonio y de bien, ha ido evolucionando con el paso del tiempo, de tal suerte que ya no sólo existen bienes de contenido exclusivamente económico, sino que existen otros llamados bienes de contenido moral o bienes morales, dentro de éstos se encuentran el derecho a la intimidad, a la reputación o mejor dicho a la tutela de ésta y el derecho a la propia imagen.

Originalmente, para definir a la personalidad y sus atributos, nos remitiríamos a conceptos propios de la doctrina civilista; sin embargo, hoy en día, la tendencia marca que se multipliquen y diversifiquen las áreas del derecho que abordan la problemática de definir, reconocer, proteger, autenticar, y salvaguardar la identidad de la persona; ejemplo de ello, son las aportaciones que al respecto hacen, Alfredo Reyes Krafft, Hans Valadez Martínez y Guillermo Tenorio Cueto, en el libro coordinado por éste último, intitulado *Los Datos Personales en México. Perspectivas y retos de su manejo en posesión de particulares*.[23]

En Francia, el derecho a la identidad, comprendida como el conjunto de características que nos distinguen de otro individuo, se recoge fundamentalmente en el Código Civil, heredado de la Declaración de los Derechos del Hombre y del Ciudadano de 1789[24].

El artículo 9º del Código Civil francés, establece el derecho al respeto de la vida privada y dota a las autoridades judiciales de toda autoridad para ejercer las medidas necesarias para preservarlo; por tanto, los derechos de la personalidad, de esencia pretoriana, son definidos como atributos de los cuales están dotados todos los seres susceptibles de derechos y obligaciones; comprendiendo su derecho al reconocimiento y respeto de su personalidad[25]. Es por ello, que diversas legislaciones alrededor del mundo, contemplan delitos en contra de la personalidad y la imagen pública, los principales actores en contra de estas actividades, dado que son los más afectados, son aquellos personajes famosos, ya sea del ámbito político o artístico, dado que un ilícito que atente contra su reputación, tiene un impacto a nivel masivo mucho más trascendente que para cualquier otro individuo, aunque no por ello menos importante.

La ley del 17 de julio de 1970, consagra la obra jurisprudencial francesa, sin dejarla inerte, por lo que los tribunales cuentan con un fuerte fundamento legal que se nutre de nuevos criterios que

[23] TENORIO CUETO, GUILLERMO (coord.), Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares, Porrúa, Universidad Panamericana, México, 2012.
[24] Aprobada por la Asamblea Nacional Francesa.
[25] DE FAULTRIER-TRAVERS Sandra, *Aspects juridiques de l ìnformation*, ESF Éditeur, Paris, 2001, p.49.

permiten mejorar la protección efectiva de la vida privada.[26] Es tal la evolución jurisprudencial al respecto, que incluso los delincuentes, cuentan con un derecho al olvido que permita su reinserción social.[27]

El interés social consagrado en el derecho a la información se ve limitado en todo momento por el derecho a la vida privada y el respecto a la personalidad; se busca que en todo momento exista una sana interacción entre ambos y que su aplicación no sea invasiva el uno del otro, sin embargo, en caso de pugna, los tribunales franceses han optado por prevalecer el derecho personal.

Los derechos de la personalidad presentan atributos muy importantes de comprender en el contexto del presente trabajo:

1. Son oponibles *erga omnes*,

2. Son intransmisibles,

3. Son personalísimos,

4. Son irrenunciables,

5. Son inembargables.

En materia de derecho autoral, constituye una infracción en materia de comercio el utilizar la imagen de una persona sin su autorización o la de sus causahabientes; gracias al análisis del artículo 73 del Reglamento de la Ley Federal del Derecho de Autor, Manuel Magaña[28] infiere que la imagen de una persona comprende tres elementos básicos:

1. *"El rostro;*

2. *Expresión corporal; y*

[26] *Ibidem.*
[27] Jurisprudencia del Tribunal de Gran Instancia de Paris del 20 de abril de 1983.
[28] MAGAÑA RUFINO, José Manuel, *Curso de Derechos de Autor en México*, Novum, México, 2013.

3. Facciones o rasgos generales, aun cuando éstos hayan sido modificados o deformados, o el nombre de la persona haya sido sustituido. Si la imagen refiere a una persona, se deberá contar con autorización de la misma[29]*."*

La identidad personal es una noción propia de las mentalidades que respetan la individualidad humana —posturas intelectuales que evitan usar a las colectividades como eje del pensamiento.

Al final de todo, cuando no tenemos nada, cuando nos miramos al espejo desnudos y en soledad sólo nos queda lo que en realidad somos, nuestra identidad. Tal y como lo expresa Viktor Frankl en su libro "El Hombre en busca de sentido", la existencia desnuda, "*Mientras esperábamos la ducha se nos hizo patente nuestra desnudez, en su sentido literal: éramos solamente un cuerpo. Nada más. Solo poseíamos la existencia desnuda*."[30]

[29] Reyes Krafft, Alfredo en NAVA GARCÉS Alberto Enrique, *La prueba electrónica en materia penal*, Porrúa, México, 2011. P. 10.
[30] Frankl, Viktor, El hombre en busca de sentido, Herder Editorial, Barcelona, 2015.

1.4 IDENTIDAD DIGITAL

Más allá de los fundamentos de genéticos, de la biología, la psicología, la sociología y en general, todos los elementos culturales que conforman la identidad humana, hoy en día podemos agregar un nuevo concepto: la identidad digital.

Es importante destacar que el concepto de identidad digital no se encuentra presente de manera exclusiva en la Internet, descrita atinada y perfectamente como ese "canal mundial de telecomunicaciones informáticas integrado por muchos canales de que a su vez, están interconectados entre sí"; luego entonces nos mantiene además de conectados y comunicados, altamente expuestos; sino también en nuestra vida diaria; por ejemplo: en la empresa, en nuestras cuentas bancarias, seguridad social y en general en casi todos los ámbitos de nuestra vida.

Esta identidad digital, se compone de diversos identificadores que generalmente son mal administrados, y en el peor de los casos, ni siquiera se tiene noción de ellos.

Hoy en día, nos encontramos inmersos en la sociedad de la información[31]; y nuestra identidad digital se convierte no sólo en nuestra llave de acceso a ella, sino la carta de presentación con la que jugamos y nos desarrollamos en ella, y como se explica a lo largo de este trabajo, la identidad digital va más allá de una simple cuestión de identificación; en efecto, justamente, gracias a la complejidad de la identidad digital, en ocasiones es difícil identificar al sujeto que se encuentra detrás de ella, quien se esconde detrás de un cierto nivel de anonimato.

Lo importante de este estudio, es profundizar a través de una metódica reflexión jurídica, que la problemática de la gestión y protección de nuestra identidad digital se compone de diversos aspectos, tanto técnicos, jurídicos, éticos, económicos e incluso psicosociales.

1.4.1 CONCEPTO Y ELEMENTOS DE NUESTRA IDENTIDAD DIGITAL.

A continuación, presento el concepto de identidad digital que hemos elaborado y sobre el cual desarrollamos este estudio y además de esto, haremos constante referencia a él a lo largo del mismo.

[31] Revista Mexicana de Ciencias Políticas y Sociales, año XLV, núm. 185, mayo-agosto de 2002. *México ante la sociedad de la información y el conocimiento. Estudio de las redes. Clasificaciones* http://www.miaulavirtual.com.mx/ciencias_sociales/Revista_UNAM/RevistaUnamPDF/RMCPYS%20NUM- 185.pdf. Consultado 20 de septiembre de 2014.

La identidad digital es el conjunto de elementos de identificación y personalización del individuo, que, de manera relativa en tiempo y dimensiones, le sirve para desenvolverse en el contexto electrónico.

La identidad digital[32], también puede ser definida como algo más profundo y de construcción constante, es decir, que se compone de los "rastros" que consciente o inconscientemente vamos dejando en el mundo digital, principalmente en nuestros navegadores, por ejemplo: nuestro historial de búsquedas, los videos que consultamos, las cookies que se alojan en nuestra computadora, los likes o me gusta en Facebook, que poco a poco van definiendo quienes somos o nuestra identidad digital.

En este punto, podemos preguntarnos válidamente, si es entonces que esta identidad no es otra cosa que una extensión de nuestra identidad del día a día, del mundo tangible, toda vez que en numerosos estudios se ha revelado que todo aquello que le sucede a nuestra identidad digital o virtual, tiene repercusiones en nuestro entorno físico, casos en los que las personas que han sido expuestas a acoso sexual a través de realidad virtual, reportan efectos psicológicos postraumáticos[3334].

Un aspecto muy relevante de los efectos reales ya sean físicos, psicológicos o emocionales que conlleva la agresión a nuestra identidad digital, un estudio de la Universidad de Stanford, realizado por Cynthia Mckelvey[35], demostró que la simple connotación sexual de los avatares femeninos de algunos juegos de video, respecto de su vestuario y apariencia, tienen un efecto negativo en la sociedad, para las mujeres representa una cosificación que las convierte en un simple objeto, y para los hombres, puede llegar a generarles la falsa justificación de una violación.

Por lo anteriormente expuesto, y por la trascendencia de comprender el alcance de la información que conforma nuestra identidad digital, dicho conjunto de elementos de identificación puede ir desde un seudónimo o nombre de usuario (el cual no siempre coincide con el real), hasta elementos que no son propios del individuo, pero pueden servir en un momento y lugar concreto para

---

[32] ERTZSCHEID, Olivier. *Qu'est-ce que l'identité numérique ? Enjeux, outils, méthodologies*. Nouvelle édition [en ligne]. Marseille : OpenEdition Press, 2013 (généré le 22 décembre 2017). En : <http://books.openedition.org/oep/332>.

[33] The Guardian, *Sexual harassment in virtual reality feels all too real – 'it's creepy beyond creepy'*. En: https://www.theguardian.com/technology/2016/oct/26/virtual-reality-sexual-harassment-online-groping-quivr Consultado el 15 de diciembre de 2016.

[34] *The Conversation, Sexual assault enters virtual reality*. En: http://theconversation.com/sexual-assault-enters- virtual-reality-67971. Consultado el 15 de diciembre de 2016.

[35] Mckelvey, Cynthia *Sexualized avatars affect the real world*, Stanford researchers find, Stanford News. En: https://news.stanford.edu/news/2013/october/virtual-female-avatars-100913.html Consultado el 15 de abril de 2014.

identificarle, como por ejemplo la dirección IP de una computadora. Es decir, que para reconocer todos aquellos elementos "identificadores", que pudiesen eventualmente formar parte de la identidad digital de un individuo, habrá que reconocerles su calidad de datos personales para que de esta manera sean correctamente tutelados.

Un sistema de identidad, ya sea real o electrónica se basa sobre el conjunto de "identificadores", en el mundo real, por ejemplo, encontramos identificadores como: nombre, apellido, fecha y lugar de nacimiento, RFC, número de seguridad social, etc.; en el mundo virtual existen otro tipo de identificadores tales como pseudónimos, correos electrónicos, avatares, etc.

Existe una categoría de identificadores otorgados por el Estado como es el caso de la CURP en México, que es una Clave Única de Registro de Población expedida por el Registro Nacional de Población, que funge como un identificador único que pretende individualizar a cada ciudadano mexicano, o bien, se reconocen como identificaciones oficiales: la credencial para votar o INE por las siglas del Instituto Nacional Electoral, que contiene diversos datos importantes como el nombre y domicilio del titular, así como su fotografía y firma; el Pasaporte, emitido por la Secretaría de Relaciones Exteriores, que contiene nombre completo, fotografía y firma, la cédula profesional con fotografía y firma, emitida por la Secretaría de Educación Pública, la Cartilla del Servicio Militar Nacional, expedida por la Secretaria de Defensa Nacional (para aquellos que la detenten), y por último, cualquier identificación oficial vigente con fotografía y firma, expedida por el gobierno federal, estatal, municipal o de la Ciudad de México.

En Estados Unidos, por ejemplo, no existe una identificación oficial nacional, es decir, en términos de la Real ID Act aprobada por el Congreso norteamericano en el año de 2005, más que una única identificación, se establecen los parámetros mínimos de datos personales que debe contener una credencial para ser considerada como válida.

Y por último, en el caso de Francia existe lo que se conoce como Carte Nationale d'Identité, que funge como una pieza de identificación a nivel nacional otorgada a todos los franceses de cualquier edad, en términos de los textos reglamentarios Décret n°55-1397 du 22 octobre 1955 relatif à la carte d'identité, Décret n°55-1397 du 22 octobre 1955 relatif à la carte d'identité , y la Circulaire du 1er mars 2010 relative à la simplification de la délivrance des cartes nationales d'identité et des passeports. Esta identificación tiene una validez de 15 años renovables, contiene elementos

fundamentales para la acreditación de la identidad en el territorio francés, tales como: apellido(s), nombre(s), fecha y lugar de nacimiento, talla, sexo, domicilio o residencia del interesado e incluso la firma y la fotografía del interesado.

Existen también, otros identificadores que sirven para la tramitación de ciertos servicios públicos como es el caso de México y la Firma Electrónica Avanzada que recientemente el SAT rebautizó como e.firma; esta e.firma es un archivo digital que identifica personas físicas y morales y que permite realizar trámites por internet en el SAT e incluso en otras dependencias del Gobierno de la República.

Está compuesta por un certificado digital que contiene una llave pública y una llave privada, utilizando criptografía asimétrica , cabe destacar que una de sus características principales es la atribución, es decir, que identifica de manera única al usuario de la misma, toda vez que para la tramitación de la misma se tuvo a la vista del agente certificador una serie de documentos que permitieron acreditar la personalidad del titular; la Firma Electrónica Avanzada, no sólo vino a revolucionar la vida de los mexicanos o extranjeros con residencia en México, no solo permitiendo que la realización de trámites a través de Internet fuera más sencilla y que la firma de contratos a distancia se pudiera optimizar; sino que además reduce significativamente la suplantación de identidad.

La biometría es otro elemento importante de nuestra identidad, ya que toma en cuenta elementos biológicos del ser humano, como lo es alguna parte de su cuerpo, que logra hacer único al individuo, actualmente se utilizan diversos métodos de identificación biométrica, el más popular sigue siendo la huella digital, aunque últimamente también se está popularizando el reconocimiento de voz y el reconocimiento facial, en general existe una larga lista de opciones: el iris, el ritmo y presión de teclado, el olor corporal, la forma de caminar, etc.

En la práctica, el uso de tecnología biométrica para la identificación de personas tiene tanto adeptos como detractores, uno de los usos más frecuentes es el control de accesos, aunque en últimas épocas ha sido utilizado también como forma de aseguramiento de transacciones bancarias o

económicas, tal es el caso de la tecnología Face ID[36] de Apple, que permite llevar a cabo compras con su cartera Apple Pay[37], o con otros proveedores como PayPal[38].

Con el alarmante incremento de casos de usurpación de identidad a nivel mundial, la identificación biométrica se convierte en una alternativa interesante, ya que cada vez se vuelve más difícil constatar mediante documentos o incluso cara a casa las identidad real de un individuo, la tecnología se abre paso como un soporte a la confianza, sin embargo, toda tecnología es susceptible de ser vulnerada y bajo ese argumento, los detractores del uso de la tecnología biométrica se oponen a que se popularice su uso, incluso integrándose a cartas de identificación nacional o pasaportes.

En México, desde el año 2016, el Sistema de Ahorro para el Retiro (SAR), implementó el uso de biométricos para que los trabajadores puedan llevar a cabo operaciones en su AFORE[39]. La incorporación de biométricos en el sistema de pensiones traerá numerosos beneficios a los trabajadores, entre los que destacan:

- Seguridad en todos los trámites del SAR al ser posible corroborar al 100% la identidad de los trabajadores, lo cual también evitará duplicidades o invasiones de las cuentas.

- Agilidad en la atención futura de los trámites pues no se requerirá de más documentación, lo cual facilitará la gestión de los formatos y solicitudes.

- Disminución de los costos de operación de los trámites para los trabajadores, al sustituir el papel por los medios electrónicos. Se estima que los gastos de gestión disminuirán entre 50 y 70 por ciento en comparación con los del papel (incluye papelería, copias, digitalización, envíos y valijas, impresiones, y captura.)

[36] Sistema de reconocimiento facial creado por la empresa Apple. En: https://support.apple.com/es-mx/HT208108. Consultado el 15 de diciembre de 2017.
[37] Sistema de pagos o cartera digital de la empresa Apple. En:https://support.apple.com/es-mx/HT208109. Consultado el 15 de diciembre de 2017.
[38] Sistema de pagos en línea que soporta transferencias de dinero entre usuarios y sirve como una alternativa electrónica a los métodos de pago tradicionales. En: https://es.wikipedia.org/wiki/PayPal. Consultado el 20 de noviembre de 2017.
[39] Administradoras de Fondos para el Retiro.

• Mayor control en los trámites, lo que inhibirá el riesgo de cualquier práctica indebida[40].

Existen otro tipo de identificadores, los que son estrictamente "virtuales", que en la mayoría de los casos fueron elegidos por las propias personas, por ejemplo, en la era del boom del correo electrónico, hace más de veinte años, cuando se popularizaron servicios como Yahoo!, Hotmail, Gmail, etc., era mucho más sencillo tener un correo electrónico con nuestro nombre o algún "alias" de nuestra predilección, hoy en día, cuando hay más de millones de cuentas de correo electrónico en el mundo, las direcciones disponibles se han acotado significativamente, sin contar el hecho de que ahora se componen de diversos caracteres alfanuméricos y caracteres especiales.

Tenemos también las cuentas de redes sociales, como Twitter, Snapchat, Pinterest, Instagram, Tinder, etc., que de igual manera nos permiten crear cuentas con nuestros datos reales, o bien, utilizar alias para guardar cierto nivel de anonimato.

Otro de los puntos fundamentales de nuestra identidad digital, son los avatares, un avatar, palabra de origen francés, presenta diferentes acepciones.

Avatar[41]: avatar [avataʀ] nom masculin

(du sanskrit, proprement « descente »)

1. Dans la religion hindouiste, Chacune des incarnations du dieu Vishnou.

2. fig. Métamorphose, transformation.

3. abusivt Mésaventure, malheur.

4. Personnage virtuel choisi par un internaute pour le représenter dans l'univers des jeux en ligne.

[40] La introducción de Biométricos en las AFORE coloca al Sistema de Pensiones a la vanguardia tecnológica del Sistema Financiero. En: https://www.gob.mx/consar/prensa/la-introduccion-de-biometricos-en-las-afore-coloca- al-sistema-de-pensiones-a-la-vanguardia-tecnologica-del-sistema-financiero-31831?idiom=es . Consultado el 7 de julio de 2016.

[41] Avatar. Diccionario Le Robert 2017.

Para nuestro estudio retendremos la última de las diferentes connotaciones que presenta en la lengua francesa, que hace mención a un personaje virtual elegido por un internauta para representarlo en el universo de los juegos en línea, sin embargo, en la lengua española, no retiene este significado:

Avatar[42]

Del fr. avatar, y este del sánscr. avatâra 'descenso o encarnación de un dios'.

1. m. Fase, cambio, vicisitud. U. m. en pl.

2. m. En la religión hindú, encarnación terrestre de alguna deidad, en especial Visnú.

3. m. Reencarnación, transformación.

De igual manera, el concepto retoma la idea de transformación, de convertirse en un algo diferente a lo que se es.

Justamente, los avatares son este conjunto de elementos que conforman nuestra identidad virtual, aquella que nos sirve para desenvolvernos en entornos digitales, para fines preferentemente lícitos, pero no limitados a éstos, es decir, que aún y cuando la creación de una identidad alterna no es en sí misma una actividad ilícita, sí puede facilitar la comisión de diversas actividades consideradas como tal, toda vez que estas identidades proporcionan a sus creadores un cierto nivel de anonimato.

El internauta vive cada vez más bajo múltiples identidades digitales, la noción de pseudonimato, contracción de pseudónimo y de anonimato, se respalda bajo el hecho de la ausencia de interacción física de los internautas.[43]

Esta identidad digital es la clave de nuestro estudio, pero sobre todo es el punto neural de la sociedad de la información y también, es la inquietud de los gobiernos al no poder identificar de una forma directa y precisa a los delincuentes informáticos que se aprovechan de esta circunstancia.

[42] Avatar; Diccionario de la lengua española (DRAE). La edición 23.a, publicada en 2014. En: http://dle.rae.es/?id=4X6SYjl consultado el 20 de noviembre de 2017.

[43] Iteanu, Olivier "*L ïdentité numérique en question*" Éditions Eyrolles, París, 2008.

La paradoja que presenta en la vida práctica esta multiplicidad de identidades, es que a pesar de ser creadas para adquirir una cierta "libertad" de acción en entornos digitales, en realidad esa noción se ve cada vez más reducida, toda vez que lejos de sentirnos libres, la administración de todos nuestros identificadores digitales impone una obligación que cada vez se vuelve más y más difícil de controlar, y precisamente esto último, es lo que pone en peligro nuestra o nuestras identidades digitales.

Dentro de los conceptos inherentes a la identidad digital, es importante definir y diferenciar unos de otros, por ejemplo: las identidades, los datos de identificación y los de autenticación.

Al crear una identidad digital, pasamos por diferentes etapas o procesos:

1. Inscripción o generación de la identidad;

2. Verificación de la creación de la cuenta o identidad;

3. Identificación;

4. Autenticación.

Por ejemplo, hoy en día contamos con una identidad digital para el desempeño de nuestras obligaciones laborales, contamos con el correo electrónico, usuario y contraseña de la empresa; pero tenemos otra identidad para desenvolvernos con familiares, amigos y desconocidos en las redes sociales. En particular el tema de las redes sociales es muy relevante en este estudio, ya que hoy en día son parte esencial de nuestro día a día.

Las redes sociales forman parte de un todo mucho más extenso, lo que se conoce como Social Media en idioma anglosajón, este universo comprende todas las herramientas a través de las cuales un individuo puede comunicarse con otros muchos en prácticamente cualquier parte del mundo[44]. Las redes sociales, son una serie de herramientas de contacto social en las cuales interactuamos a través de un perfil, ya sea real o imaginario, es decir un usuario, alias o avatar, que a su vez puede comprender una serie de identificadores, por ejemplo: un perfil de Twitter, comprende un usuario,

[44] Mokhtari, Farah " L ' impact des réseaux sociaux», Telecom Sud Paris. En: http://ima4505.wp.tem-tsp.eu/files/2012/03/impactreseauxsociaux.pdf consultado el 20 de septiembre de 2017.

una biografía, una fotografía o espacio para una imagen, un medio de contacto, y en ocasiones hasta la fecha de nacimiento, para aquellos usuarios que desean dar a conocer ese dato.

fig. 1 Ejemplo de un perfil de Twitter

En otras redes sociales mucho más complejas, se recaban otra serie de identificadores que pueden incluso llegar a ser considerados como datos sensibles, por ejemplo, Facebook; la información que se expone en esta red social, basándonos tan sólo en su formulario de datos personales, incluye aspectos tan delicados e íntimos como la preferencia sexual, el estado civil, la afiliación política y hasta la religión, además de un cúmulo de información que se va incorporando a nuestro perfil día con día.

La importancia de estas redes sociales es que nos permiten interactuar con otros individuos cercanos y lejanos con quien podemos tener un sin fin de relaciones de diversos tipos, sin embargo, en este punto entra un concepto por demás interesante, eso que se conoce como la vida privada social, aunque suene contradictorio, el ser humano tiene ese derecho a la confidencialidad respecto de sus datos personales y a la vez, ese derecho a "salir de sí mismo para convivir con otros"[45], lo cual debe

[45] Marguénaud, J-P. « *La Courte européenne des droits de l'homme* », 5e éd. Coll. Connaissance du droit, Dalloz, 2011, p.82.

ser garantizado de manera plena, es decir, respetar su voluntad de inscribirse en una red social garantizando la protección y confidencialidad de sus datos personales.

Tan sólo en 2014, México era el principal usuario de redes sociales en Latinoamérica y en comparación con diversos países del mundo, siendo Facebook la red social más popular:

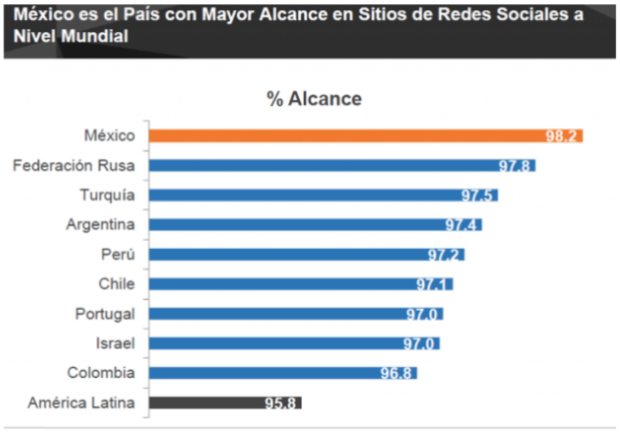


fig. 2 Estadística elaborada por Comscore, publicada por Forbes México.[46]

En el caso de Francia, el uso de redes sociales desde el 2012 ha ido en repunte tal y como se muestra en la siguiente gráfica:

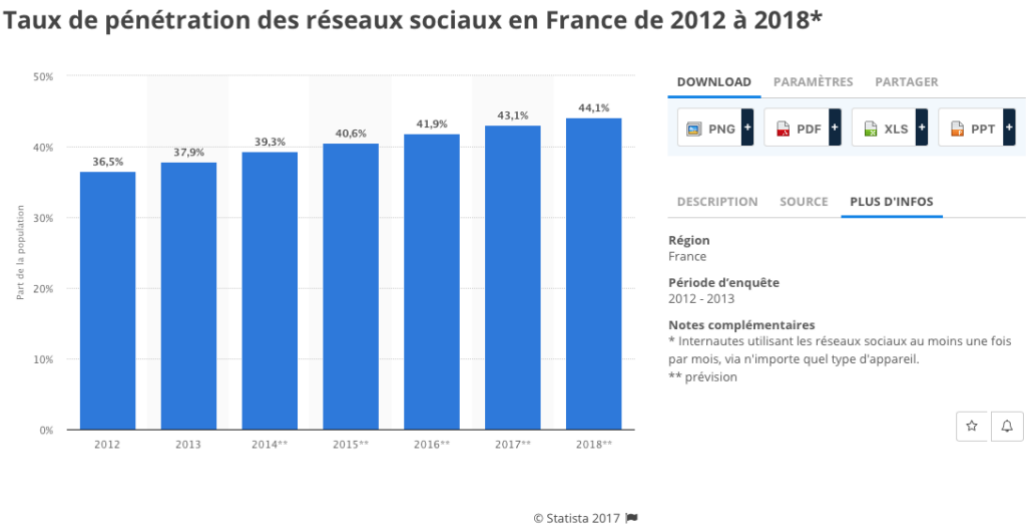


fig. 3 Tasa de penetración de las redes sociales en Francia de 2012 a 2013 y la previsión a 2018[47].

[46] México, primer lugar en penetración Social Media. En: https://www.forbes.com.mx/mexico-primer-lugar-en-penetracion-social-media/. Consultado el 30 de septiembre de 2014.

[47] Taux de pénétration des réseaux sociaux en France de 2018-2018. En:

Es innegable que la mayoría de los proveedores de las redes sociales más populares en el mundo son de origen estadounidense, en estos casos, cuando el usuario se inscribe a estas redes sociales se adhiere a los contratos estipulados por el proveedor, los cuales son de carácter civil y mercantil, sin embargo, en diferentes procesos judiciales se ha comprobado que estos contratos son violatorios de diversas leyes incluyendo cláusulas abusivas[48] y dejando en estado de indefensión a los usuarios de estas plataformas.

Cuando un usuario se inscribe a una red social residente en el extranjero, normalmente ese contrato fijará como jurisdicción aquel país, que generalmente suele ser Estados Unidos, en este caso, a pesar de que bajo las reglas del derecho civil y los principios básicos de los contratos esto sería suficiente para que ambas partes estén claras de sus derechos y excepciones a los mismos; existen derechos irrenunciables, como son los derechos del consumidor o el derecho al respecto a la vida privada y a la protección de datos personales.

El derecho americano, permite la existencia de los contratos efectuados a través de medios electrónicos en dos diferentes modalidades, el "*click wrap*" y el "*browse wrap*", el primero requiere que el usuario llene una casilla y en el segundo caso basta con que el usuario visite el sitio para entender que cuenta con el consentimiento de los términos y condiciones de uso del sitio; en México, el Código Civil Federal reconoce el consentimiento efectuado a través de medios electrónicos como consentimiento expreso. Mediante este tipo de mecanismos de presunción o evidencia de la expresión del consentimiento, es que operan la mayoría de las plataformas de redes sociales.

1.5 LA IDENTIDAD SOCIAL

Ya que hemos hablado del derecho a la protección de datos personales, es importante tocar el derecho a decidir el nivel de exposición social del individuo, ya que, en este sentido, es capaz, al menos en teoría, de medir los riesgos que esto último conlleva, el decir, el equilibrio de dos conceptos interesantes el *privacy by design* y el *sociability by design*.

El concepto de identidad social, aparece de forma reiterada en la jurisprudencia de la Corte

https://fr.statista.com/statistiques/490928/utilisateurs-reseaux-sociaux-france/

[48] Cláusula abusiva en: http://www.rtl.fr/actu/futur/facebook-juge-par-la-justice-francaise-qu-implique-cette-decision-pour-le-reseau-social-7776909636 consultado el 15 de mayo de 2015.

europea de los derechos del hombre, esta identidad es opuesta a la identidad física, ya que la identidad social es una especie de pasaporte que refleja lo mejor de su personalidad, es decir, estamos hablando del perfil social, ese que nos permite desempeñarnos en la sociedad de la información.

Este perfil se convierte en una especie de vitrina personal, mediante la cual el usuario de redes sociales, decide libremente qué es lo que quiere revelar o no, de su verdadera identidad y de los aspectos más íntimos de su personalidad.

Una de las principales razones por las cuales las personas se enganchan con el uso de las redes sociales, es inherente a la necesidad de compartir y convivir a través de esta interconexión fomentada y lograda gracias a las nuevas tecnologías. Los lazos que el usuario puede establecer, son de naturaleza diversa, y en efecto, pueden tener diferentes connotaciones para éste, por ejemplo: dar o recibir un *poke*[49] [50], un *like*[51], o de forma más reciente, expresar una emoción concreta respecto de una publicación con la ayuda de lo que se conoce como emoticón[52], les ha dado a las redes sociales un sentido mucho más íntimo y personal. La sociedad mexicana, por ejemplo, es demasiado sensible al tema de recibir o no recibir aprobaciones o reacciones respecto de sus publicaciones, tan es así que hay personas que auténticamente pueden sufrir ansiedad o angustia[53] por la indiferencia de sus amigos de *Facebook*.

Otra interesante función a destacar dentro de las redes sociales más populares y que implica un claro tratamiento de datos personales, no siempre consentido por el titular, es la famosa *etiqueta* o *tag*, que consiste en la identificación de personas o usuarios, ya sea en una publicación o directamente en una fotografía, esto cobra relevancia porque no existe una autorización *a priori* por

[49] *Poke* o *toque*, se refiere a la función de la red social *Facebook*, que permite de alguna manera llamar la atención del usuario al que se le da ese toque, aún y cuando puede tener una connotación de *saludo*, en exceso puede llegarse a convertir en un tipo de acoso.

[50] Hipertextual, *Poke: la funcionalidad de Facebook que sirve para… nada*. En: https://hipertextual.com/archivo/2010/07/poke-la-funcionalidad-de-facebook-que-sirve-para-nada/ consultado el 20 de febrero de 2015.

[51] *Like* o *me gusta*, es una función de la red social *Facebook*, que originalmente se ilustraba como una mano con el pulgar arriba, lo que en lenguaje anglosajón se conoce como *Thumbs up* he históricamente se utiliza como sinónimo de aprobación, posteriormente se añadieron otro tipo de emociones ligadas a la publicación de algún usuario. Como referencia, consultar: https://elsemanario.com/hasta-el-momento/122803/video-likes-con-emociones-llegan-a-facebook/

[52] Emoticono es un neologismo que proviene de emoción e icono. El plural es emoticonos. En algunos países y comunidades de Internet se denominan emoticones (latinización de la palabra en inglés emoticon), emoticón, iconos gestuales o caretas. En: https://es.wikipedia.org/wiki/Emoticono Consultado el 20 de abril de 2017.

[53] Diario Vanguardia, *El 25.3 de los mexicanos sabe o conoce a alguien que siente angustia y tristeza cuando nadie les comenta, comparte o reacciona a sus publicaciones*. En: https://www.vanguardia.com.mx/articulo/estas-son-las-emociones-que-has-percibido-al-no-recibir-likes-en-facebook Consultado el 10 de abril de 2016.

parte de la persona que ha sido identificada o referida, la opción que tiene generalmente, es la de remover dicha etiqueta o que ésta no aparezca en su biografía, siendo una expresión muy clara del sistema norteamericano respecto del tratamiento de datos personales o lo que se conoce como *opt out* que presume el consentimiento hasta en tanto no se manifieste la oposición.

Por último, antes de cerrar el tema controversial de las redes sociales, mencionaremos el último concepto que consideramos un tanto banalizado y a la vez peligroso, el término *amigo*, en *Facebook*, todos aquellos usuarios que forman parte de tu lista de contactos, son identificados como *amigos*, en Twitter por ejemplo, se conocen como *seguidores*, que es un concepto menos íntimo; el hecho de que aquellas personas (reales o ficticias) que se añaden a la lista de contactos de esta red social sea denominada como *amigo*[54], puede llegar a ser una potencial arma contra la privacidad y seguridad de los usuarios.

Los *conceptos* tradicionales respecto de las relaciones interpersonales de los individuos han tomado otra dimensión gracias a las redes sociales; por ejemplo, hoy en día se puede suponer que una relación amorosa es algo formal por el hecho de publicarla como tal en Facebook, de hecho, la jurisprudencia francesa se ha pronunciado respecto de la supresión del estatus *comprometido* y la probable causal de pago de daños y perjuicios y daño moral.

Lo relevante de comprender el alcance de aquello tan incomprendido e imperceptible como es nuestra identidad digital es poder medir los riesgos de nuestra exposición, de tal suerte que podamos limitar todo aquello que compartimos de nosotros hacia el mundo.

CAPÍTULO II.
EL PRINCIPIO DE PROTECCIÓN DE LOS DATOS PERSONALES.

La protección de datos personales es un concepto a geometría variable entre los tres países que son parte de nuestro estudio, ya que los principios rectores de este importante derecho, no siguen los mismos criterios en estas diferentes tradiciones jurídicas; mientras que en Estados Unidos existe un principio muy acotado de protección de datos personales, en Europa, es un tema bastante regulado,

[54]Gros, Marie-Joëlle, *Professeur, veux-tu être mon ami ?* En: http://www.liberation.fr/ecrans/2011/02/08/professeur-veux-tu-etre-mon-ami_955813 consultado del 23 de mayo de 2014.

por lo tanto, la ley francesa también cuenta con reglas muy claras en la materia; en el caso de México, la legislación respeta cabalmente los criterios europeos de protección de los datos personales pero prevé un sistema de excepciones muy precisas que la hacen compatible con la normativa estadounidense.

Comenzaremos con Estados Unidos, por ser el país, cuyo sistema de protección es mucho más laxo.

2.1 LA VISIÓN ESTADOUNIDENSE DE LA PROTECCIÓN DE DATOS PERSONALES.

En Estados Unidos, históricamente y más aún desde el 11 de septiembre de 2001[55], existen fuertes prioridades como la seguridad nacional[56] que sin lugar a dudas se encuentra muy por encima del derecho a la privacidad. Sobre todo, debemos tomar en cuenta que la protección constitucional de este derecho es limitada, toda vez que lo más importante dentro de la sociedad norteamericana no es el individuo como sujeto de derechos sino en función de su rol social, porque lo más importante es la seguridad y bienestar de la nación como un todo. Los ciudadanos estadounidenses pueden invocar protección mediante la Cuarta Enmienda y la Ley de Privacidad, pero los derechos de protección de datos otorgados en el sector de la aplicación de la ley se interpretan de manera limitada con una tendencia general a privilegiar la aplicación de la ley y los intereses de seguridad nacional; en particular, todo aquello que tiene que ver o que justifique el intercambio y transferencia de información de carácter personal, aún en contra de la voluntad o el desconocimiento del titular de ésta.

Cabe recordar que la denominada FISA o *Foreign Intelligence Surveillance Act*, de 1978, creada originalmente, para que sólo en caso de manera justificada pudiese existir vigilancia electrónica gubernamental en contra de poderes extranjeros o espías residentes en los Estados Unidos, ha sufrido muchas enmiendas que permiten la recolección de información de inteligencia no clasificada, incluso el Congreso autorizó en el año de 2008 que fueran sujetas a vigilancia personas residentes fuera del territorio estadounidense, situación que se ratificó en 2012 y que sigue vigente hasta este 2017 y seguramente no dejará de estarlo.

---

55 *How has national security changed since 9/11/2001?* En: https://www.securitydegreehub.com/national-security-since-september-eleventh/ consultado el 11 de enero de 2017.

56 Brown, Logan, *A Brief History of American National Security*. En: https://ivn.us/2014/03/24/a-brief-history-of-americas-approach-to-security/ consultado el 13 de septiembre de 2013.

Es preciso remarcar que aún y cuando se requiera de una orden judicial para llevar a cabo esta vigilancia y obtención de información, es relativamente sencillo encuadrar alguna de las causales que permita obtener esta orden, anteponiendo la salvaguarda de la seguridad nacional.

No obstante, se dice que los derechos civiles de las personas no están siendo del todo minados. La Junta de Supervisión de las Libertades Civiles y la Privacidad (PCLOB)[57], en 2014, luego de una exhaustiva revisión, emitió un informe completo y público sobre la Sección 702 que abordaba ciertas inquietudes de privacidad, concluyendo finalmente que el programa gubernamental de la Sección 702 opera dentro de las limitaciones legales, recopila información valiosa y está bien administrado y es efectivo en proteger la seguridad nacional.

El PCLOB señaló específicamente que, "Hasta la fecha, no hay casos conocidos en los que el personal del gobierno violó deliberadamente el estatuto, los procedimientos de selección o los procedimientos de minimización". En ese informe, el PCLOB hizo una serie de recomendaciones al gobierno con la intención de mejorar las garantías de privacidad y libertades civiles en el programa de la Sección 702. En febrero de 2016, el PCLOB informó que todas sus recomendaciones habían

[57] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Jul. 2, 2014), https://www.pclob.gov/library/702-Report.pdf
The PCLOB recommendations were:

- NSA's targeting procedures should require written statements regarding the expected foreign intelligence value of collection against particular targets (Recommendation 1);
- FBI's minimization procedures should more clearly reflect FBI's U.S. person querying practices (Recommendation 2);
- Additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters (Recommendation 2);
- NSA and CIA queries of Section 702 information using U.S. person query terms (*i.e.*, identifiers) should be accompanied by a written explanation of the reasonable likelihood the query will return foreign intelligence (Recommendation 3);
- A random sampling of tasking sheets, as well as NSA and CIA U.S. person query terms, should be submitted annually to the FISC to assist in the FISC's consideration of the FISA Section 702 certification renewals (Recommendation 4);
- Any rules governing the conduct of the Section 702 program should be incorporated into the annual certification process to the extent the FISC agrees that those rules are mandatory (Recommendation 5);
- NSA should continue to periodically assess the availability of additional or more advanced filtering techniques for "upstream" and for "about" collection (Recommendations 6 and 7);
- The government should publicly release the current Section 702 minimization procedures used by the CIA, FBI and NSA (Recommendation 8);
- The government should work to develop metrics for Congress and for public release providing additional insight about the extent to which NSA acquires and uses the U.S. persons information incidentally acquired through the Section 702 program (Recommendation 9); and
- The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs (Recommendation 10).

sido implementadas total o parcialmente por el gobierno. Aun así, sigue existiendo una deficiencia considerable con respecto al nivel de privacidad y protección de datos personales en comparación con los países de la Unión Europea e incluso con México.

Es menester examinar las reglas más relevantes de los Estados Unidos sobre protección de datos. Ciertamente se vuelve compleja la aplicación de la ley federal y las disposiciones de seguridad nacional al tiempo que se excluyen las leyes a nivel estatal y local. En esencia, los principios generales de protección de datos derivados de la Cuarta Enmienda a la Constitución de EE. UU., La Ley de Privacidad de 1974 y las salvaguardas establecidas en relación con las leyes que facultan a las agencias de aplicación de la ley para procesar datos con el fin de cumplir con sus tareas. Estas garantías se pueden encontrar en la Ley de Privacidad de Comunicaciones Electrónicas, la Ley de Vigilancia de Inteligencia Extranjera, la Ley de Comunicaciones Internas, la Ley de Comunicaciones Almacenadas, la Ley de Registro de Perforaciones o la Ley PATRIOTA de los EE. UU.

Con el fin de presentar la evolución de los derechos de privacidad en los EE. UU., Se analizan las nuevas acciones legislativas que modifican secciones de las leyes antes mencionadas. La atención se centra en el Anteproyecto de Ley de reparación judicial de 2015 y en la Ley FREEDOM de 2015. Cabe destacar que el término "aplicación de la ley" generalmente se refiere a las actividades de las agencias responsables de la prevención, detección e investigación de delitos y la ejecución de sanciones penales. Para cumplir con este deber, las autoridades policiales confían en el permiso para poder recopilar, usar y difundir datos personales (procesar datos personales). El grado en que las actividades de procesamiento de datos califican como una actividad de aplicación de la ley depende de la interpretación de "delito". El término puede usarse de una manera estrecha o amplia. El contenido del crimen puede estar limitado al delito común o incluir todas las formas de delito. La última interpretación abarcaría explícitamente actividades delictivas que amenazan la seguridad nacional.

Recientemente, se ha tenido noticia de que el gobierno de los Estados Unidos a través de su agencia de Inteligencia[58], recopila información de prácticamente cualquier sujeto, dentro y fuera de su territorio nacional a través de las redes sociales, es decir, que ya no sólo se encuentra en riesgo nuestra *identidad digital* sino nuestra *identidad social*, no sólo se trata de quiénes somos, sino de

[58] *CIA Tech Firm Seeks More Social Media Spying.* En: https://www.usnews.com/news/articles/2016-04-15/cia-tech-firm-seeks-more-social-media-spying consultado el 20 de junio de 2016.

dónde nos movemos, con quién convivimos, de qué platicamos u opinamos, y en general una radiografía de nuestras relaciones personales.

2.1.1 CUARTA ENMIENDA A LA CONSTITUCIÓN DE LOS ESTADOS UNIDOS

Las garantías constitucionales de protección de datos en el contexto de la aplicación de la Ley son muy limitadas. La principal fuente constitucional que sirve de base para la protección legal contra las acciones intrusivas de aplicación de la ley en este campo es la Cuarta Enmienda a la Constitución. Se entiende que su garantía del ""derecho de las personas a estar seguras en sus personas, casas, documentos y efectos, contra registros e incautaciones irrazonables" abarca ciertos datos atribuidos a una persona, tales como registros telefónicos o bancarios". Sin embargo, solo se aplica en los casos en que el individuo tiene una "expectativa legítima de privacidad"; este concepto se ha reducido de manera exhaustiva para excluir todos los casos en que un individuo haya entregado voluntariamente la información en cuestión a terceros, como su banco o servicio telefónico. proveedor, antes de que por motivo de aplicación de la ley, la autoridad se apodere de esta información (*Third Party Doctrin*[59]) . Esto efectivamente excluye áreas amplias de datos personales de la protección de la Cuarta Enmienda, tales como sitios web visitados, destinatarios de correo electrónico, números de teléfono marcados, así como servicios públicos, bancos, y registros de educación. Otro grave problema es que la Cuarta Enmienda generalmente no se aplica a ciudadanos y residentes extranjeros, como ciudadanos de la Unión Europea que no residen en los EE. UU.

En los casos limitados en los que se aplican las garantías de la Cuarta Enmienda, pueden justificarse por intereses gubernamentales "razonables". Si se constata que las garantías prevalecen, las reparaciones equivalen a la supresión como prueba en los procesos penales y en los recursos civiles.

2.1.2 LA LEY DE PRIVACIDAD DE 1974

La Ley de Privacidad de 1974[60] tiene como objetivo regular el procesamiento de datos personales en los EE. UU. Regula la recopilación, uso y divulgación de muchos tipos de información personal, que se describe como un *registro* que se guarda respecto de un individuo: "que incluye, entre otros, su

[59] M. Thompson II, Richard, *The Fourth Amendment Third-Party Doctrine*. En: https://fas.org/sgp/crs/misc/R43586.pdf consultado el 20 de agosto de 2014.
[60] Ley de Privacidad de 1974. En: https://www.justice.gov/opcl/privacy-act-1974 consultado el 15 de diciembre de 2015.

educación, transacciones financieras, historial médico y antecedentes penales o laborales"; así como "su nombre, o el número de identificación, símbolo u otro particular de identificación asignado al individuo, como un dedo, una huella de voz o una fotografía".

En principio, sus destinatarios son todo tipo de agencias federales, incluidas las agencias encargadas de hacer cumplir la ley, que excluyen a las agencias estatales o locales y entidades privadas. El tema de la Ley de Privacidad de 1974 se limita a los registros mantenidos en un *sistema de registros*[61], es decir, una base de datos que se describe como un "grupo de registros bajo el control de cualquier agencia de la cual se recupera información con el nombre del individuo o por algún número de identificación, símbolo u otro particular identificativo asignado al individuo ". Esto debería abarcar los usos más comunes de los datos en el contexto de la aplicación de la ley, pero probablemente excluya las actividades de extracción de datos. Solo algunos datos, específicamente los considerados como sensibles, se tratan de manera preferencial, en particular los derechos de la Primera Enmienda, relacionados con la libertad de expresión y asociación, y los registros médicos y psicológicos. La aplicación de la Ley está limitada a ciudadanos estadounidenses o extranjeros con residencia permanente en los Estados Unidos.

Con respecto a las reglas de divulgación, "ninguna agencia divulgará ningún registro que esté contenido en un sistema de registros por ningún medio de comunicación a ninguna persona u otra agencia, excepto de conformidad con una solicitud por escrito o con el consentimiento previo por escrito de, el individuo al que pertenece el registro". Sin embargo, la aplicación de esta regla está sujeta a doce excepciones enumeradas explícitamente, en resumen, *uso rutinario* y para divulgación a otras agencias y jurisdicciones gubernamentales de los EE. UU. *para una aplicación de la ley civil o actividad criminal*. Esto reduce en gran medida el impacto de esta garantía para un individuo en el contexto de la aplicación de la Ley.

Una persona disfruta del derecho de acceder y revisar sus datos y conservar una copia de los mismos; puede solicitar su revisión si cree que los datos no son precisos, relevantes, oportunos o completos. Sin embargo, se excluye el acceso a cualquier información *compilada con una anticipación razonable de una acción o procedimiento civil*, lo que limita efectivamente los derechos de acceso.

[61] *a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.* 5 U.S.C. § 552a(a)(5).

Los requisitos de transparencia incluyen la obligación de cada agencia de informar a las personas de las que solicita datos de la autorización de dicha solicitud, el propósito principal de la recopilación de datos, los usos de rutina y los efectos que pueden producirse en el interesado. Además, debe publicarse un aviso en el Registro Federal sobre la existencia y el sistema de registros establecido por una agencia. Sin embargo, las obligaciones de transparencia están parcialmente limitadas por una prueba de razonabilidad en beneficio de la agencia interesada.

Las agencias están obligadas a mantener en sus registros solo dicha información sobre las personas *según sea relevante y necesaria para cumplir el propósito de la agencia que se requiere cumplir por ley o por orden ejecutiva del presidente*. Se realizan para garantizar la precisión y relevancia, puntualidad e integridad de los registros, *según sea razonablemente necesario para garantizar la equidad para el individuo* en cuestión. Los elementos de relevancia y necesidad se pueden entender como una especie de prueba de proporcionalidad. Sin embargo, la Ley no menciona explícitamente dicho término. o requiere un equilibrio de intereses.

La referencia a *un propósito* insinúa un principio de limitación de propósito, pero ha sido aplicado por los tribunales de una manera bastante débil, haciendo hincapié en que *un* (más bien entendido como *cualquiera*) propósito legítimo de la agencia pertinente es suficiente. Los tribunales parecen aplicar una interpretación más estricta en el campo del *uso rutinario* de los registros, que requiere un *uso de dicho registro que sea compatible con el propósito para el que fue recopilada*. Los tribunales deciden caso por caso, cuando tal principio sea violado, dado que solo se aplica en el contexto del uso rutinario, sin embargo, no llega a ser un principio legal general.

Finalmente, aun y cuando las agencias están obligadas a mantener la seguridad y confidencialidad de los registros que conservan, no existen disposiciones con respecto a los períodos de retención de datos.

Además de las sanciones penales para los funcionarios de la agencia o empleados que violen las garantías contenidas en la subsección 5 U.S.C. § 552a (i) de la Ley, los recursos civiles son la herramienta principal de las personas que desean invocar una violación de sus derechos en virtud de la Ley.

La Ley garantiza cuatro tipos de acciones legales disponibles para individuos:

1. Cuando una agencia toma la determinación de *no enmendar el registro de un individuo de acuerdo con su solicitud, o no realiza dicha revisión de conformidad con* las reglas de procedimiento;

2. Se niega a cumplir con la solicitud de una persona de acceder a sus registros;

3. *no mantiene ningún registro con respecto a cualquier persona con tal precisión, relevancia, puntualidad y exhaustividad como sea necesario para garantizar la imparcialidad en cualquier determinación relacionada con las calificaciones, el carácter, los derechos o las oportunidades o los beneficios para el individuo que puede hacerse sobre la base de dicho registro y, en consecuencia, se toma una determinación que es adversa para el individuo*; o

4. En general, *no cumple con ninguna otra disposición de esta sección* [es decir la Ley], *o cualquier norma promulgada en virtud de la misma, de tal manera que tenga un efecto adverso en un individuo*.

Bajo estos cuatro tipos de acción legal, si se encuentra a favor del individuo, los tribunales le otorgarán al individuo una enmienda de sus registros, más los honorarios del abogado y otros costos del litigio; acceso a sus registros, más honorarios de abogados y otros costos de litigio; y daños reales con un mínimo de USD 1,000, más el costo de la acción junto con los honorarios razonables de los abogados.

Finalmente, debe mencionarse que la Ley prevé la instalación de funcionarios internos que supervisen el cumplimiento de las obligaciones de privacidad, que, sin embargo, por su propia naturaleza como funcionarios internos, no tienen la misma independencia estructural y poderes que las Autoridades Europeas de Protección de Datos o la Autoridad mexicana.

Por último, tocando justamente el tema de las restricciones a la protección de la privacidad y de la protección de los datos personales so pretexto de la seguridad nacional, es importante destacar que como se vio anteriormente, las garantías de protección de datos de los Estados Unidos ya permiten amplias excepciones en el sector de la aplicación de la Ley. En los últimos años se han

promulgado numerosas leyes adicionales que permiten la recopilación de datos por parte de las autoridades, con fines de investigaciones de seguridad nacional y/o criminal, que restringen aún más las garantías generales de protección de datos. El número de disposiciones legales emitidas es abrumador, lo que dificulta dar una visión general completa de la situación legal. Entre las más importantes o preocupantes están: la Ley de Vigilancia de Inteligencia Extranjera (FISA), la Ley de Privacidad de Comunicaciones Electrónicas (ECPA) y la Ley PATRIOTA de los EE. UU. Con motivo de esta última Ley fueron enmendadas principalmente la FISA y el ECPA. Sin embargo, muchas de sus disposiciones inicialmente limitadas en el tiempo han sido reautorizadas por sucesivas reformas, más recientemente por la Ley FREEDOM de EE. UU.

2.1.3 LA LEY FREEDOM DE 2015

La Ley FREEDOM[62], que reforma diferentes disposiciones de la Ley Patriota, es una de las más intrusivas de la historia de este país, ya que permite a las autoridades federales la creación de registros personales, vigilancia electrónica, el uso de *pen register*[63], utilizar dispositivos de trampa y rastreo[64], así como cualquier otra forma de obtención de información relacionada con actividades de inteligencia extranjera, contraterrorismo, y propósitos criminales, entre otros. El grave problema del término *otros propósitos*, es justamente que casi cualquier actividad podría encuadrarse en esta categoría, y, por lo tanto, cualquier individuo nacional o extranjero puede ser espiado en aras de la seguridad nacional.

La Ley FREEDOM, entre otras cosas, autoriza la recopilación masiva de registros telefónicos y se modificaron después de alcanzar su fecha de vencimiento el 1 de junio de 2015. Las reglas del subcapítulo IV facultan al FBI para acceder a ciertos registros comerciales y cualquier cosa tangible en relación con una actividad de investigación relacionada con la aplicación de la ley, que se encuentra dentro del marco de 50 U.S.C. § 1861. La solicitud de acceso debe tener como objetivo

[62] *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015'' or the ''USA FREEDOM Act of 2015.* En: https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048enr.pdf consultado el 20 de febrero de 2016.

[63] Un registro de bolígrafo o registrador de número marcado (DNR) es un dispositivo electrónico que registra todos los números llamados desde una línea telefónica particular. El término ha llegado a incluir cualquier dispositivo o programa que realice funciones similares a un registro de pluma original, incluidos los programas que supervisan las comunicaciones de Internet.

[64] El término *dispositivo de trampa y rastreo* significa un dispositivo o proceso que captura los impulsos electrónicos entrantes u otros que identifican el número de origen u otra información de marcación, ruteo, direccionamiento y señalización razonablemente probable para identificar la fuente de un cable o comunicación electrónica, siempre que, sin embargo, dicha información no incluya el contenido de ninguna comunicación.

obtener información de inteligencia extranjera de una persona ajena a los EE. UU. o proteger contra el terrorismo internacional o actividades de inteligencia clandestina.

La información obtenida sobre personas no estadounidenses se puede compartir con otros para cualquier propósito legal. Un prerrequisito necesario para recopilar la información es la aprobación de un juez. Solo si la autoridad judicial determina que la solicitud presentada por el FBI cumple con los requisitos, se puede acceder a los registros comerciales. La solicitud del FBI puede hacerse ante un juez del Tribunal FISA o un Juez Magistrado estadounidense designado.

En caso de ser aprobada, la aplicación debe tener un contenido específico, que se describe en 50 USC § 1861 (b) (2). Con respecto a este contenido, la promulgación de la Ley FREEDOM ha llevado a cambios considerables que también afectan las normas de protección de datos.

De acuerdo con la versión anterior de 50 U.S.C. § 1861, la solicitud de una orden de cobro debía contener una declaración de hechos que demostrara que existen motivos razonables para creer que las evidencias buscadas eran relevantes para una investigación legítima y una enumeración de los procedimientos de minimización adoptados por el Fiscal General.

La ley FREEDOM introduce una estructura diferente y nuevas condiciones con respecto al contenido de una orden de búsqueda al agregar dos párrafos más. La primera modificación requiere un "término de selección específico que se utilizará como base para la producción de los elementos tangibles buscados". La segunda modificación es la introducción de un procedimiento independiente para la recopilación de registros de detalles de llamadas en una base continua en el subpárrafo. Este nuevo subpárrafo especifica el contenido de la declaración de hechos, si los registros de detalles de llamadas se proporcionarán al FBI de manera continua. Entonces, en todos los casos, un término de selección específico debe ser presentado por el FBI en su solicitud de una orden de búsqueda. Esta condición se aplica independientemente de la ciudadanía y tiene como objetivo evitar la recopilación masiva de datos dentro de los EE. UU. Para aumentar la claridad de estas disposiciones, la Ley FREEDOM da una definición de este término recientemente introducido, básicamente, un término de selección específico significa un dato que identifica específicamente a una persona, cuenta, dispositivo personal, dirección o cualquier otro identificador específico.

2.1.4 LA LEY COOPA *Children's Online Privacy Protection Act of 1998*

En 1998, el Congreso de los Estados Unidos de América, aprueba una reforma a las reglas aplicables en materia de comercio para los menores de 13 años, ese justamente es el antecedente legal y restrictivo de las redes sociales como Facebook que no permiten a los menores de 13 años contar con un perfil en redes sociales, claro, esto de buena fe, porque no existe un procedimiento para constatar que efectivamente el menor que pretende inscribirse a éstas, supera la edad legal mínima requerida, ya que el proveedor únicamente está obligado a llevar a cabo su mejor esfuerzo basado en las mejores prácticas.

La Sección 312.4 (d) identifica la información que debe ser divulgada por los proveedores de servicios en internet en su política de privacidad en línea. Si bien la Regla original exigía que los operadores proporcionaran amplias categorías de información en sus avisos de privacidad en línea, la Regla enmendada ahora adopta un enfoque más corto y simplificado para cubrir las prácticas de recopilación y uso de información más críticas para los padres. Según la Regla enmendada, el aviso en línea debe indicar las siguientes tres categorías de información:

- El nombre, la dirección, el número de teléfono y la dirección de correo electrónico de todos los operadores que recopilan o mantienen información personal a través del sitio o servicio (o, después de enumerar todos esos operadores, brindan la información de contacto que manejará todas las consultas de los padres);

- Una descripción de qué información recopila el operador de los niños, incluso si el operador les permite a los niños poner su información personal a disposición del público, cómo el operador usa dicha información y las prácticas de divulgación del operador para dicha información; y

- Que el padre puede revisar o haber eliminado la información personal del niño y negarse a permitir su posterior recolección o uso, y establecer los procedimientos para hacerlo. ("aviso en el sitio web o servicio en línea").

Al agilizar los requisitos de notificación en línea de la Regla, la Comisión espera alentar a los operadores a proporcionar descripciones claras y concisas de sus prácticas de información, que pueden tener el beneficio adicional de ser más fáciles de leer en pantallas más pequeñas (por

ejemplo, en teléfonos inteligentes u dispositivos móviles).

La última enmienda define *información personal* para incluir identificadores, como un número de cliente almacenado en una cookie, una dirección IP, un procesador o número de serie del dispositivo o un identificador único del dispositivo que se puede usar para reconocer a un usuario a lo largo del tiempo diferentes sitios web o servicios en línea, incluso cuando dicho identificador no está correlacionado con otros elementos de información personal. Por lo tanto, deberá divulgar en su política de privacidad y en su aviso directo a los padres, su recopilación, uso o divulgación de tales identificadores a menos que no recopile ninguna otra *información personal* y que dichos identificadores se recopilan a través de su sitio o servicio con el único propósito de proporcionar *soporte para las operaciones internas* de su sitio o servicio.

Una de las medidas más importantes de esta enmienda es el empoderamiento y control parental respecto de la información de los menores que los proveedores u operadores pueden tratar.

La enmienda requiere que los operadores hagan esfuerzos razonables, teniendo en cuenta la tecnología disponible, para garantizar que el o los padres de un niño reciban una notificación directa de las prácticas del operador con respecto a la recopilación, uso o divulgación de información personal de los niños, incluida la notificación de cualquier cambio o actualización a las prácticas a las cuales el padre consintió previamente. La reforma cambió significativamente el formato y el contenido de la información que debe incluirse en el aviso directo a los padres de un operador. Ahora proporciona una hoja de ruta muy detallada de qué información se debe incluir en su aviso directo, dependiendo de qué información personal se recopila y con qué fines.

Hay cuatro casos en que se requiere un aviso directo en términos de esta reglamentación:

1. Cuando un operador busca obtener el consentimiento verificable de un padre antes de la recopilación, uso o divulgación de la información personal de un niño. En este caso, el aviso directo debe:

    a) Indicar que el operador ha recopilado la información de contacto en línea del padre del niño y, si ese es el caso, el nombre del niño o el padre, para obtener el consentimiento del padre;

b) Indicar que se requiere el consentimiento del padre para la recopilación, el uso o la divulgación de dicha información, y que el operador no recopilará, usará o divulgará ninguna información personal del niño si el padre no proporciona dicho consentimiento;

c) Indicar los elementos adicionales de información personal que el operador tiene la intención de recopilar del niño, o las posibles oportunidades para la divulgación de información personal, si el padre proporciona el consentimiento;

d) Contener un hipervínculo al aviso en línea del operador sobre sus prácticas de tratamiento de información (es decir, su política de privacidad);

e) Proporcionar los medios por los cuales el padre puede proporcionar un consentimiento verificable para la recopilación, el uso y la divulgación de la información; y por último

f) Indicar que si el padre no proporciona el consentimiento dentro de un tiempo razonable desde la fecha en que se envió el aviso directo, el operador eliminará la información de contacto del padre.

2. Cuando un operador busca voluntariamente proporcionar un aviso a un padre de las actividades en línea de un niño que no impliquen la recopilación, el uso o la divulgación de información personal. En este caso, el aviso directo debe:

a) Indicar que el operador ha recopilado la información de contacto en línea del padre del niño para avisar y posteriormente informar al padre sobre la participación de un niño en un sitio web o servicio en línea que de otro modo no recopila, usa o divulga información personal de los niños;

b) Indicar que la información de contacto en línea de los padres no será utilizada o divulgada para ningún otro propósito;

c) Indique que el padre puede negarse a permitir la participación del niño en el sitio web o servicio en línea y puede requerir la eliminación de la información de contacto en línea de los padres y cómo pueden llevarlo a cabo los padres; y

d) Proporcione un hipervínculo al aviso en línea del operador sobre sus prácticas de información.

3. Cuando un operador tiene la intención de comunicarse con el niño varias veces a través de la información de contacto en línea del niño y no recopila ninguna otra información. En este caso, el aviso directo debe:

a) Indicar que el operador ha recopilado la información de contacto en línea del niño para llevar a cabo múltiples comunicaciones en línea;

b) Indicar que el operador ha recogido la información de contacto en línea del padre del niño para notificar a los padres que el niño se ha registrado para recibir múltiples comunicaciones en línea del operador;

c) Indicar que la información de contacto en línea recopilada del niño no se usará para ningún otro propósito, ni se revelará, ni se combinará con ninguna otra información recopilada del niño;

d) Indique que el padre puede negarse a permitir un mayor contacto con el niño y solicitar la eliminación de la información de contacto en línea del padre y del niño, y cómo pueden hacerlo los padres;

e) Indique que, si el padre no responde a este aviso directo, el operador puede usar la información de contacto en línea recopilada del niño para el propósito indicado en el aviso directo; y

f) Proporcionar un hipervínculo al aviso en línea del operador sobre sus prácticas de información.

4. Cuando el propósito del operador para recolectar el nombre de un niño y su padre y la información de contacto en línea sea para proteger la seguridad de un niño y la información no se usa o divulga para ningún otro propósito. En este caso, el aviso directo debe:
    a) Indicar que el operador ha recopilado el nombre y la información de contacto en línea del niño y el padre para proteger la seguridad de un niño;

    b) Indicar que la información no se usará ni divulgará por ningún motivo no relacionado con la seguridad del niño;

    c) Indicar que el padre puede negarse a permitir el uso, y requerir la eliminación, de la información recopilada, y cómo los padres pueden hacerlo;

    d) Indicar que, si el padre no responde a este aviso directo, el operador puede usar la información para el propósito indicado en el aviso directo; y

    e) Proporcione un hipervínculo al aviso en línea del operador sobre sus prácticas de información.

2.2 EL SISTEMA MEXICANO DE PROTECCIÓN DE DATOS PERSONALES

La protección de datos personales en México, surge como una necesidad de equiparar nuestro derecho al de la sociedad europea, en parte por los tratados de libre comercio y en parte por la clara necesidad de contar con una normativa federal en la materia. Como analizaremos más adelante, respecto de la evolución de nuestro derecho mexicano en materia de protección de datos personales, después de más de diez años, nuestra Ley Federal de Protección de Datos Personales en Posesión de los Particulares, pudo por fin ver la luz tal y como la conocemos.

El modelo conocido como *híbrido*, es fruto de intensas negociaciones en las Cámaras legislativas y de la inspiración de normativas internacionales tales como: la Directiva 95/46/CE del parlamento europeo, el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC), las Directrices de la OCDE sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales, el Convenio 108 del Consejo de Europa para la protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y los Estándares

Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal (Resolución de Madrid).

Luego de discutir los diferentes proyectos de Ley, al final se optó por crear un modelo que combinara lo mejor de cada una de las disposiciones anteriormente citadas, por diversas razones, una de ellas, de carácter inminentemente económica; dado que nuestro entonces socio comercial más fuerte era Estados Unidos, y la legislación de este último es laxa y sectorial.

Era menester respetar los acuerdos anteriormente pactados en el Tratado de Libre Comercio de América del Norte, respecto al libre flujo transfronterizo de bienes, servicios y capitales, y los datos personales que van aparejados en estas transacciones; sin embargo, era imprescindible contar con un marco legal en materia de privacidad y protección de datos, y así fue como entre negociaciones y malabares de la industria, los legisladores y la sociedad civil, se creó un precedente mundial que promoviera a la vez la protección de los datos personales y el desarrollo comercial del país.

La Ley mexicana, así como la francesa, está basada en principios y deberes que rigen al tratamiento de datos personales, aunque estos se encuentran mucho más detallados que en la normativa europea.

En el tema de la protección a la identidad es fundamental vincular cada principio con el derecho a la protección a la identidad, que como ya hemos mencionado, está conformada por un sin fin de datos de carácter personal, desde aquellos que dan origen al propio individuo como lo es el código genético, hasta aquellos que son menos transcendentales como el domicilio o el teléfono de contacto, hasta los datos que se van generando en el día a día con nuestras actividades en Internet, en particular, aquellos metadatos que contienen referencias cada vez más precisas respecto de nuestra identidad.

La legislación mexicana, retoma los principios rectores en la Unión Europea y Francia, y de alguna manera los desenrolla creando así ocho principios rectores y dos deberes con el mismo nivel de exigibilidad.

Estos principios son los siguientes:

2.2.1. EL PRINCIPIO DE LICITUD

El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares define este principio de la siguiente manera:

Artículo 10. El principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.

Es muy importante destacar que la legislación mexicana reconoce la competencia y aplicación de la normativa y las reglas del derecho internacional, por lo que no es de sorprenderse que en repetidos casos el INAI ha atraído a su jurisdicción diversos casos relacionados con el tratamiento de datos personales de ciudadanos mexicanos que se han visto vulnerados en plataformas de origen extranjero como el caso de la empresa Sony[65] y el de UBER[66]; esto cobra relevancia ya que en ambos casos se vieron comprometidos datos financieros o patrimoniales, situación que pone en evidente riesgo de sufrir daños patrimoniales a los usuarios de las citadas plataformas, ya sea por la venta de los datos de pago (número de tarjeta de crédito, fecha de vencimiento, nombre del titular, CVV) en el mercado negro, o peor aún, por la usurpación de identidad de los titulares de los medios de pago para poder comprar bienes o servicios en su nombre o clonar las tarjetas para poder bajar recursos directamente en un cajero automático.

2.2.2 EL PRINCIPIO DE INFORMACIÓN

Este principio, que no admite excepción, se ve consagrado principalmente en el Aviso de Privacidad, sin embargo, es la evidencia más clara del derecho constitucional consagrado en el artículo 16 de nuestra Carta Magna, el derecho a la autodeterminación informativa.

En la mayoría de los casos de usurpación de identidad, se observa como antecedente un tratamiento ilícito de datos personales, ya sea por la inexistencia de un aviso de privacidad, que de

[65]El Instituto Federal de Acceso a la Información y Protección de Datos se estrenó con Sony por el 'hackeo' a la base de datos de PlayStation http://expansion.mx/tecnologia/2011/05/10/el-ifai-se-estrena-con-sony
[66] INAI solicita a Uber información sobre hackeo revelado la semana pasada http://www.cioal.com/2017/11/27/inai-uber-hackeo/

primera instancia permita identificar al responsable del tratamiento de los datos personales y por ende deja al titular de estos sin la posibilidad de conocer qué se pretende hacer con ellos, cuál es la finalidad para la que se recaban y cómo constatar qué y cuántos datos personales están siendo objeto de este tratamiento.

En términos de la Ley y su Reglamento, el principio de información es una obligación primordial que debe ser llevada a cabo de la siguiente manera:

Artículo 15 de la LFPDPPP: El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.

2.2.2.1. ARTÍCULOS APLICABLES DEL REGLAMENTO

Artículo 23. El responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales a través del aviso de privacidad, de conformidad con lo previsto en la Ley y el presente Reglamento.

2.2.2.2. CARACTERÍSTICAS DEL AVISO DE PRIVACIDAD

Artículo 24. El aviso de privacidad deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.

2.2.2.3. MEDIOS DE DIFUSIÓN

Artículo 25. Para la difusión de los avisos de privacidad, el responsable podrá valerse de formatos físicos, electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular.

Por lo anteriormente expuesto y en relación con el tema que nos compete del tratamiento ilícito de datos personales, en particular el fenómeno de la usurpación de identidad, confirmamos que en la mayoría de los casos su génesis proviene de un inexistente o deficiente aviso de privacidad, en violación directa al principio de información.

A pesar de que la entrada en vigor de la Ley se dio hace más de siete años en nuestro país, es una realidad que hay muy pocos responsables, ya sean personas físicas o morales, que cuentan con un buen aviso de privacidad, fruto de un análisis profundo del tipo de datos que se tratan, de las finalidades para las que se recaban y se llega a un listado concreto y realista de la información que efectivamente se procesa; por ejemplo, muchas empresas que recaban datos biométricos tales como la huella digital o la fotografía de una persona, no lo declaran en el texto del aviso de privacidad, y por experiencia sabemos que el mal uso de estos elementos identificadores podría dar lugar a que fuesen utilizados posteriormente para usurpar la identidad de una persona.

2.2.3. EL PRINCIPIO DE CONSENTIMIENTO

La llave de acceso al tratamiento de datos personales de forma lícita es el consentimiento de su titular. La ley mexicana, a diferencia de la mayoría de legislación europea, prevé la posibilidad de operar y recabar datos personales que no sean de carácter sensible o patrimonial a través del consentimiento tácito, es decir, que con sólo tener evidencia de que se puso a disposición del titular el aviso de privacidad y el titular no se manifestó en contra de lo declarado en dicho documento, se entiende que consiente que se lleve a cabo el tratamiento de sus datos personales en términos de lo declarado en dicho aviso.

2.2.3.1 CARACTERÍSTICAS DEL CONSENTIMIENTO

En términos del Reglamento (RLFPDPPP), el consentimiento sobre el tratamiento de datos personales, debe tener características primordiales y esenciales para respetar este derecho fundamental del titular, de lo contrario, el responsable podría ser sancionado por no poder acreditar la correcta obtención del consentimiento.

> "Artículo *12. La obtención del consentimiento tácito o expreso deberá ser:*
>
> *I. Libre: sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular;*
>
> *II. Específica: referida a una o varias finalidades determinadas que justifiquen el tratamiento, y*

III. *Informada: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.*

El consentimiento expreso también deberá ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento."

Asimismo, el responsable determinará claramente si por el tipo de datos personales que pretende tratar, debe de recabar el consentimiento expreso del titular o bastará con presumir el consentimiento tácito del mismo.

2.2.3.2. CONSENTIMIENTO TÁCITO

Artículo 13 del RLFPDPPP. "*Salvo que la Ley exija el consentimiento expreso del titular, será válido el consentimiento tácito como regla general…"*

2.2.3.2.1. SOLICITUD DEL CONSENTIMIENTO TÁCITO

En términos del RLFPDPPP, el momento oportuno para hacer del conocimiento del titular el aviso de privacidad por parte del responsable, debe ser previo al tratamiento de los datos personales, es decir, previo a que se recaba la información, es decir que el principio de consentimiento va estrechamente ligado al principio de información.

En particular, cuando se trate de datos que no son considerados como sensibles o patrimoniales, los responsables podrán solicitar el consentimiento tácito en los términos siguientes:

"Artículo 14. Cuando el responsable pretenda recabar los datos personales directa o personalmente de su titular, deberá previamente poner a disposición de éste el aviso de privacidad, el cual debe contener un mecanismo para que, en su caso, el titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular.

En los casos en que los datos personales se obtengan de manera

indirecta del titular y tenga lugar un cambio de las finalidades que fueron consentidas en la transferencia, el responsable deberá poner a disposición del titular el aviso de privacidad previo al aprovechamiento de los datos personales. Cuando el aviso de privacidad no se haga del conocimiento del titular de manera directa o personal, el titular tendrá un plazo de cinco días para que, de ser el caso, manifieste su negativa para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular. Si el titular no manifiesta su negativa para el tratamiento de sus datos de conformidad con lo anterior, se entenderá que ha otorgado su consentimiento para el tratamiento de los mismos, salvo prueba en contrario.

Cuando el responsable utilice mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que le permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en ese momento se deberá informar al titular sobre el uso de esas tecnologías, que a través de las mismas se obtienen datos personales y la forma en que se podrán deshabilitar."

Es decir, que para los casos en los que opere el consentimiento tácito como manifestación de la voluntad del titular para el tratamiento de sus datos personales, y cuando no se recaben los datos de manera personal bastará con que el responsable indique en el propio aviso de privacidad los medios mediante los cuáles podrá manifestar su negativa al tratamiento de sus datos para las finalidades secundarias.

2.2.3.3. CONSENTIMIENTO EXPRESO

El consentimiento expreso en términos el artículo 1803 del Código Civil Federal se define como:

"Artículo 1803.- El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:

I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología,

o por signos inequívocos…"

Es decir, el consentimiento expreso consiste en una expresión de la conducta humana que se caracteriza por la manifestación de signos inequívocos que indican que el sujeto está conforme o acepta, en este caso, el tratamiento de su información.

La legislación federal mexicana reconoce como medios para manifestar el consentimiento expreso, los verbales, escritos, los medios electrónicos o cualquier otro que permita la tecnología, siempre y cuando no haya lugar a duda de la aceptación. Sin embargo, en los siguientes párrafos describiremos qué características específicas debe tener para cumplir con la legislación en materia de protección de datos personales.

En términos de nuestra legislación en materia de protección de datos personales, el responsable debe de obtener el consentimiento expreso en los siguientes casos contemplados en el reglamento:

"Artículo 15…

I. Lo exija una ley o reglamento;
II. Se trate de datos financieros o patrimoniales;
III. Se trate de datos sensibles;
IV. Lo solicite el responsable para acreditar el mismo, o
V. Lo acuerden así el titular y el responsable."

En este sentido, cuando el responsable se ubique en cualquiera de los supuestos anteriormente descritos, deberá solicitar el consentimiento expreso de manera que no incumpla ningún otro principio.

Como mencionamos anteriormente y para detallar lo que Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los particulares, el consentimiento verbal y escrito se definen de la siguiente manera:

"Consentimiento verbal

Artículo 18. Se considera que el consentimiento expreso se otorgó verbalmente cuando el titular lo externa oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral.

Consentimiento escrito

Artículo 19. Se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. Tratándose del entorno digital, podrán utilizarse firma electrónica o cualquier mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento."

Cabe recordar que contar con evidencia de la obtención del consentimiento expreso del titular, siempre será una carga para el responsable, por lo que al momento de que el responsable defina los procesos para la solicitud del consentimiento expreso por parte del titular, se deberá tener en cuenta los esfuerzos y mecanismos para obtener y guardar la evidencia de la expresión de dicho consentimiento.

2.2.3.4. EXCEPCIONES AL CONSENTIMIENTO

El principio de consentimiento prevé ciertas excepciones, que, de ubicarse en dichos supuestos, el responsable no estará obligado a obtener el consentimiento del titular para el tratamiento de sus datos personales. Dichas excepciones están contempladas en el artículo 10 de la LFPDPPP.

"Artículo 10.- No será necesario el consentimiento para el tratamiento de los datos personales cuando:

I. Esté previsto en una Ley;

II. *Los datos figuren en fuentes de acceso público;*

III. *Los datos personales se sometan a un procedimiento previo de disociación;*

IV. *Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;*

V. *Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;*

VI. *Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o*

VII. *Se dicte resolución de autoridad competente."*

Respecto de las excepciones anteriormente descritas, cabe aclarar que el principio de información no prevé excepción alguna, como ya vimos, es por ello que siempre deberá ponerse a disposición del titular, por cualquier medio, el aviso de privacidad; y respecto de los datos que figuren en fuentes de acceso público, es aún más importante dar a conocer el aviso de privacidad para que los titulares se encuentren en aptitud de oponerse a la continuación del tratamiento de datos personales.

Lo que podemos concluir de este principio básico, es que se traduce en la puerta de acceso y autorización al tratamiento de datos personales en México, y que además de ello, funciona como llave de paso para regular el uso y divulgación de la información de carácter personal cara al responsable.

2.2.4. EL PRINCIPIO DE CALIDAD

El principio de calidad es uno de los más complejos en la práctica, ya que amerita una constante vigilancia y correcta administración de las bases de datos, cosa que se complica a medida que el volumen de datos personales se incrementa.

En términos del Reglamento, este principio consiste en:

> *"Artículo 36. Se cumple con el principio de calidad cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.*
>
> *Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular, y hasta que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga.*
>
> *Cuando los datos personales no fueron obtenidos directamente del titular, el responsable deberá adoptar medidas razonables para que éstos respondan al principio de calidad, de acuerdo con el tipo de datos personales y las condiciones del tratamiento.*
>
> *El responsable deberá adoptar los mecanismos que considere necesarios para procurar que los datos personales que trate sean exactos, completos, pertinentes, correctos y actualizados, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación."*

Es decir, que el principio de calidad está estrictamente ligado al correcto mantenimiento de las bases de datos, sea cual sea el medio de tratamiento de estos, es decir, medios físicos como el papel o medios electrónicos como discos duros de computadora.

Aunque parece tarea fácil, como lo mencionamos al principio de esta sección, la puesta en marcha del principio de calidad se vuelve mucho más compleja conforme aumenta el volumen de datos que trata el responsable, es por ello que siempre debe operar un criterio de minimización, incluso jugando a favor del responsable, quien, al tratar una menor cantidad de información, reducirá la carga de trabajo ligada al cumplimiento del principio de calidad.

Ahora bien, a efecto de reducir la cantidad de datos que el responsable tiene bajo su custodia, y también en atención a la proporcionalidad y finalidad del tratamiento, deberán establecerse plazos de conservación perfectamente identificados, para tal efecto, el RLFPDPPP, al respecto menciona:

> *"Plazos de conservación de los datos personales*
>
> *Artículo 37. Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento, y deberán atender las disposiciones aplicables a la materia de que se trate, y tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos en su posesión previo bloqueo de los mismos, para su posterior supresión.*

Asimismo, el reglamento también establece reglas para generar los procedimientos de conservación, bloqueo y supresión de los datos personales:

> *"Procedimientos para conservación, bloqueo y supresión de los datos personales*
>
> *Artículo 38. El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales, que incluyan los periodos de conservación de los mismos, de conformidad con el artículo anterior.*
>
> *Prueba del cumplimiento de los plazos de conservación*

Artículo 39. Al responsable le corresponde demostrar que los datos personales se conservan o, en su caso, bloquean, suprimen o cancelan cumpliendo los plazos previstos en el artículo 37 del presente Reglamento, o bien, en atención a una solicitud de derecho de cancelación.

Como hemos podido constatar el principio de calidad, obliga claramente al responsable a llevar a cabo al menos las siguientes tareas:

a) Identificar las leyes que le son aplicables por el ramo de la industria al que pertenezca y así identificar los plazos de conservación que dichas leyes le impongan;

b) Establecer procesos y procedimientos eficaces para el bloqueo y supresión de la información; y

c) Documentar todos aquellos procedimientos seguros de destrucción de información y generar evidencia del bloqueo y la supresión de los datos personales.

2.2.5. EL PRINCIPIO DE FINALIDAD

Cada uno de los datos personales que el responsable recabe de los titulares por cualquier medio, de manera directa o indirecta, deberá estar ligado a una finalidad clara y legítima, dichas finalidades deberán citarse expresa y claramente en el aviso de privacidad, en cumplimiento del artículo 12 de la Ley.

"Artículo 12.- El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular."

Las disposiciones de la Ley, se complementan con las del reglamento, que detallan

de forma más precisa cómo deben de identificarse y catalogarse las finalidades del tratamiento de datos personales.

"Principio de finalidad

Artículo 40. Los datos personales sólo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad, en términos del artículo 12 de la Ley.

Para efectos del párrafo anterior, la finalidad o las finalidades establecidas en el aviso de privacidad deberán ser determinadas, lo cual se logra cuando con claridad, sin lugar a confusión y de manera objetiva se especifica para qué objeto serán tratados los datos personales.

Diferenciación de finalidades

Artículo 41. El responsable identificará y distinguirá en el aviso de privacidad entre las finalidades que dieron origen y son necesarias para la relación jurídica entre el responsable y el titular, de aquellas que no lo son.

Oposición del tratamiento para finalidades distintas

Artículo 42. El titular podrá negar o revocar su consentimiento, así como oponerse para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular, sin que ello tenga como consecuencia la conclusión del tratamiento para estas últimas finalidades.

Tratamiento para finalidades distintas

Artículo 43. El responsable no podrá llevar a cabo tratamientos para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, a menos que:

I. Lo permita de forma explícita una ley o reglamento, o

II. El responsable haya obtenido el consentimiento para el nuevo tratamiento.

2.2.6. EL PRINCIPIO DE LEALTAD

El principio de lealtad, pretende garantizar al titular de los datos personales, que el responsable no utilice medios engañosos o fraudulentos para recabar el consentimiento respecto del tratamiento de sus datos personales.

"Principio de lealtad

Artículo 44. El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, en los términos establecidos en el artículo 7 de la Ley.

No se podrán utilizar medios engañosos o fraudulentos para recabar y tratar datos personales. Existe una actuación fraudulenta o engañosa cuando:

I. Exista dolo, mala fe o negligencia en la información proporcionada al titular sobre el tratamiento;

II. Se vulnere la expectativa razonable de privacidad del titular a la que refiere el artículo 7 de la Ley, o

III. Las finalidades no son las informadas en el aviso de privacidad."

En la práctica, el principio de lealtad es uno de los más comúnmente violados en el ámbito de Internet, las redes sociales y las aplicaciones móviles. La mayoría de las aplicaciones móviles, e incluso los sistemas operativos de las grandes empresas, llevan a cabo prácticas poco éticas al momento de informar y recabar el consentimiento de sus usuarios; coaccionan, por decirlo de alguna manera, a sus usuarios a aceptar sus políticas de privacidad y términos y condiciones de uso, aún y cuando son claramente violatorios de los derechos de protección de datos personales, a

efecto de ejemplificar uno de los casos más comunes, en seguida reproducimos los términos y condiciones del sistema operativo iOS:

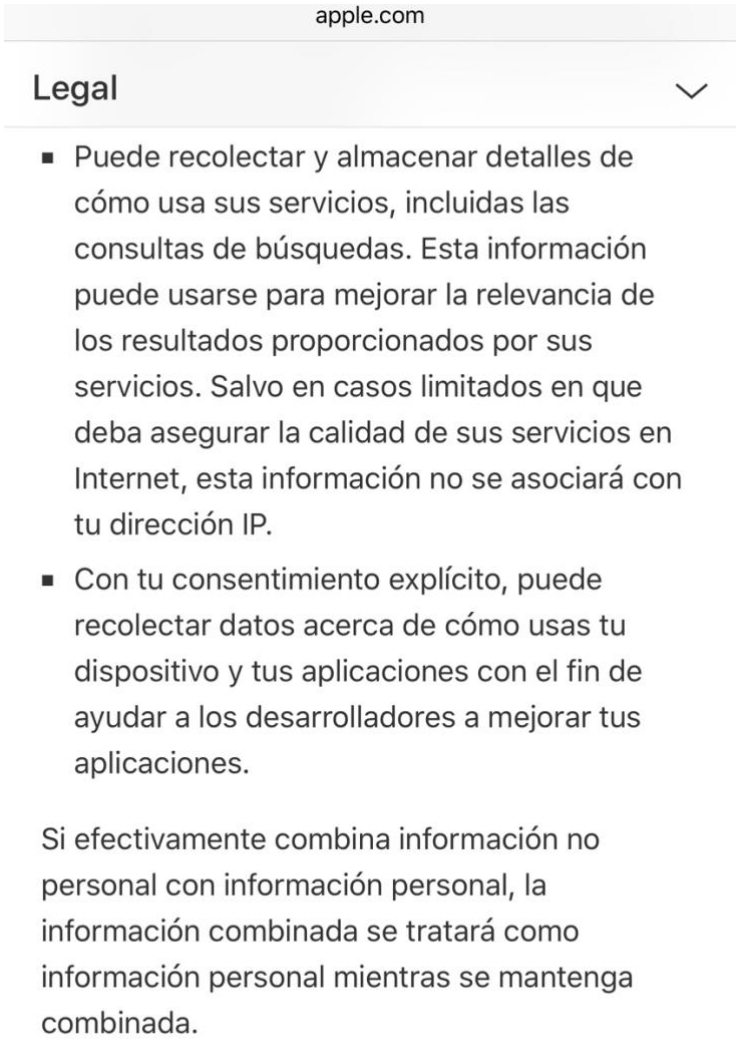


Fig. 4 Política de Privacidad iOS 11.2

Aún y cuando "menciona" que el tratamiento de algunos datos personales se hará únicamente con el consentimiento del titular, en realidad, al momento de actualizar el sistema operativo, se exige que el usuario acepte los términos y condiciones de uso, así como la política de privacidad para poder descargar la nueva versión.

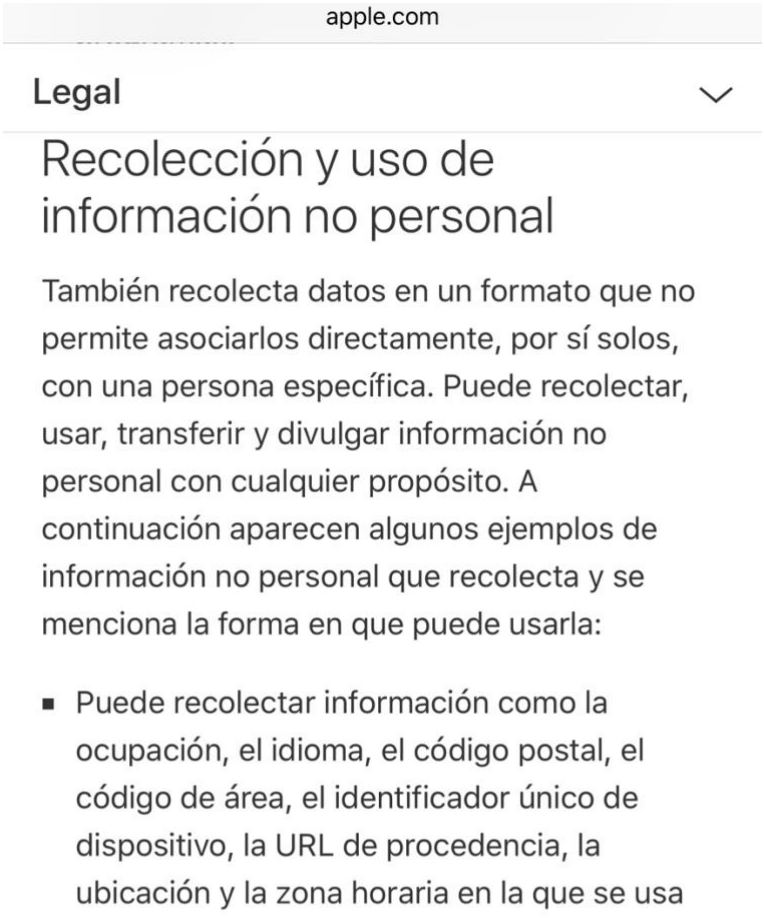


Fig. 5 Política de Privacidad iOS 11.2

Fig. 6 Política de Privacidad iOS 11.2

Aun y cuando las pantallas anteriores muestran que la política de privacidad de Apple es violatoria de diversos principios de la LFPDPPP, el que claramente se ve transgredido es el de lealtad ya que dicha política encuadra en las tres fracciones del artículo 44 del Reglamento.

2.2.7. EL PRINCIPIO DE PROPORCIONALIDAD

El principio de proporcionalidad, que también se encuentra presente en la legislación europea, obliga al responsable del tratamiento de los datos personales, a recabar, y en general, realizar tratamiento de aquella información que sea estrictamente indispensable para llevar a cabo sus operaciones, este principio va de la mano con el de minimización, aún y cuando este segundo en realidad forma parte del primero.

Como hemos podido constatar en el resto de los principios contemplados por la legislación mexicana, todos van estrechamente relacionados y forman parte del sistema de protección de datos en nuestro país, en este caso, el principio de finalidad, ya que cada dato que se solicite,

debe de ir estrechamente relacionado con las finalidades declaradas en el aviso de privacidad y más aún, que se justifiquen con base en las actividades objetivas de la empresa; es decir que si por ejemplo, un médico recaba datos personales para poder brindar sus servicios de salud, no se justificaría que solicitara datos financieros para poder ofrecer en un futuro pólizas de seguros de gastos médicos menores.

El reglamento dispone lo siguiente en relación con este principio:

> *"Principio de proporcionalidad*
>
> *Artículo 45. Sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido.*
>
> *Criterio de minimización*
>
> *Artículo 46. El responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar."*

2.2.8. EL PRINCIPIO DE RESPONSABILIDAD

El principio de responsabilidad, se hereda de las legislaciones anglosajonas, derivado de la palabra en inglés *accountability*, una de las acepciones de esta palabra, es responsabilidad, aunque en realidad va mucho más allá, ya que implica la obligación de un individuo u organización de dar cuenta de sus actividades, aceptar la responsabilidad por ellas y divulgar los resultados de manera transparente.

Otra de las acepciones de esta palabra, que ha sido adoptada por la CNIL, es: la responsabilidad se refiere a la obligación de las empresas de implementar mecanismos y procedimientos internos para demostrar el cumplimiento de las normas de protección de datos[67].

La ley mexicana, contempla una serie de obligaciones, en ocasiones poco claras para el

[67] Accountability, glosaire CNIL en: https://www.cnil.fr/fr/glossaire

responsable, que además se extienden hasta los encargados, que se encuentran comprendidas en este principio, que conlleva velar y responder por el correcto tratamiento de datos personales; pero básicamente consiste en:

> *"Artículo 47 del RLFPDPPP. En términos de los artículos 6 y 14 de la Ley, el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano.*
>
> *Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines."*

Tal y como lo contempla el último párrafo, el responsable y también el o los encargados dentro del ámbito de su competencia, podrán implementar políticas internas que se ajusten a estándares internacionales, para ello el INAI (Instituto Nacional de Acceso a la Información Pública y Protección de Datos), en el año de 2015, publicó una tabla de equivalencia funcional entre estándares de seguridad y la legislación mexicana[68].

En esta tabla, se desarrolla un mapeo de los principales estándares internacionales en materia de seguridad y gestión de la información; sin embargo, no es una tarea tan sencilla de llevar a cabo, por ello desarrollamos el tema de forma más precisa en la tercera parte de este trabajo, pero a efecto de comprender la correcta dimensión del volumen de tareas que implica la implementación práctica de este principio.

El artículo 60, del RLFPDPPP, a la letra indica:

[68] Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su reglamento y las recomendaciones en materia de seguridad de datos personales. En: http://inicio.inai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2015).pdf consultado el 20 de septiembre de 2016.

"El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores:

I. El riesgo inherente por tipo de dato personal;

III. La sensibilidad de los datos personales tratados;

IV. El desarrollo tecnológico, y

V. Las posibles consecuencias de una vulneración para los titulares.

De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:

I. El número de titulares;

II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;

III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y

IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable."

Parece tarea sencilla, pero no lo es, de la simple redacción anteriormente señalada, se derivan muchas preguntas para el responsable, sobre todo si tomamos en cuenta que muchos de éstos

son pequeñas y medianas empresas, *startup*[69] o profesionales independientes ¿cómo y por dónde comenzar?, ¿no son acaso tareas que parecen demasiado técnicas?, ¿requiero contratar a un profesional para que me asesore con esto o es que podré hacerlo de manera independiente?

El Reglamento también esclarece un poco el panorama, para dar cumplimiento, al menos en el tema de la seguridad de los datos personales, en el siguiente artículo:

> *"Artículo 61. A fin de establecer y mantener la seguridad de los datos personales, el responsable deberá considerar las siguientes acciones:*
>
> *I. Elaborar un inventario de datos personales y de los sistemas de tratamiento;*
>
> *II. Determinar las funciones y obligaciones de las personas que traten datos personales;*
>
> *III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;*
>
> *IV. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;*
>
> *V. Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;*

[69] *Empresa emergente, compañía emergente, compañía de arranque y compañía incipiente. En:* https://es.wikipedia.org/wiki/Empresa_emergente consultado el 20 de agosto de 2017.

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;

VII. Llevar a cabo revisiones o auditorías;

VIII. Capacitar al personal que efectúe el tratamiento, y

IX. Realizar un registro de los medios de almacenamiento de los datos personales.

El responsable deberá contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores."

Además de ello, define los diferentes tipos de medidas a implementar:

"Medidas para el principio de responsabilidad

Artículo 48. En términos del artículo 14 de la Ley, el responsable deberá adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.

Entre las medidas que podrá adoptar el responsable se encuentran por lo menos las siguientes:

I. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable;

II. Poner en práctica un programa de capacitación, actualización y concientización del personal

sobre las obligaciones en materia de protección de datos personales;

III. *Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad;*

IV. *Destinar recursos para la instrumentación de los programas y políticas de privacidad;*

V. *Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así́ como para mitigarlos;*

VI. *Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran;*

VII. *Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales;*

VIII. *Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así́ como de sanciones por su incumplimiento;*

IX. *Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y el presente Reglamento, o*

X. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento."

2.2.9. EL DEBER DE SEGURIDAD

El cumplimiento del deber de seguridad, es independiente al principio de responsabilidad, pero se encuentran estrechamente ligados, cabe recordar que en términos de la LFPDPPP:

"Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico."

Para el cumplimiento de este deber, el responsable deberá proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, lo que significa en caso de que se suceda una vulneración de este deber, entonces deberán actualizarse y perfeccionarse las medidas implementadas ya que ha quedado en evidencia la falta de eficacia de las mismas.

2.2.10. EL DEBER DE CONFIDENCIALIDAD

Hablando de este deber, es preciso remitirnos al concepto de confidencialidad, este proviene de la palabra confianza, es decir, que alguien ha proporcionado a otro, información en el marco de

una relación de confianza, por lo cual, el receptor deberá conservar la reserva de lo hecho o dicho por el informante[70].

En términos de la Ley:

> *"Artículo 21.- El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable."*

Hasta hace algunos años, los convenios de confidencialidad, principalmente se visualizaban como un mecanismo de protección de secretos industriales o desarrollos en materia de propiedad intelectual de una persona física o moral; con la entrada en vigor de la LFPDPPP y su Reglamento, los convenios o contratos de confidencialidad han tenido que evolucionar para contemplar también la reserva en el tratamiento de datos personales que se ha confiado tanto a responsables como encargados y en algunos casos, también a terceros.

Algo muy interesante es que la evolución del ámbito de aplicación de los convenios de confidencialidad implica que la violación a la reserva de la información, podría ocasionarle al infractor, no sólo consecuencias de carácter civil, por el incumplimiento contractual, sino también infracciones de carácter administrativo e incluso penal.

2.3 LOS PRINCIPIOS RECTORES DE LA PROTECCIÓN DE DATOS PERSONALES EN FRANCIA.

En Francia, la legislación en materia de protección de datos personales es la Ley de Informática y Libertades o Ley nº 78-17 del 6 de enero de 1978 [71] (LIL). Cabe señalar que este texto ha sido reformado en numerosas ocasiones, de hecho, la reforma más reciente de 2017, se da con motivo de la reforma al reglamento general de protección de datos europeo (GDPR)[72].

[70] Confidencial, adjetivo. En: http://dle.rae.es/?id=AFGgKxB. Consultado el 2 de enero de 2017.
[71] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[72] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such

La Ley nº 78-17 del 6 de enero de 1978, es una de las primeras en haber regulado el tratamiento de datos personales en Europa. En términos del artículo 2 de la citada Ley, que posteriormente fuera modificado para ajustarse a la Directiva Europea de 1995, el ámbito de aplicación estaba delimitado al tratamiento de datos personales llevado a cabo a través de medios automatizados o no automatizado, o cuya vocación era integrar expedientes, con excepción de aquellos datos que fueran recopilados y tratados para fines exclusivamente personales.

Existen conceptos básicos que debemos analizar de manera previa al estudio de los principios, ya que es menester el comprender lo que la Ley nº 78-17 del 6 de enero de 1978 entiende como dato personal, expediente y el alcance de la palabra tratamiento.

Dato personal[73]: En términos del artículo 2º de la LIL, constituye un dato personal, toda información relativa a una persona física identificada o que pueda ser identificada, directa o indirectamente ya sea por referencia a un número de identificación o a uno o más elementos que le correspondan. Para determinar si una persona es identificable en estos términos, se debe considerar el conjunto de medios disponibles que permitan su identificación o bien, a los que el responsable del tratamiento o cualquier otra persona pueda tener acceso.

Es importante destacar que incluso si los datos personales que se traten, puedan gozar de un cierto nivel de anonimato, si éste puede ser reversible, entonces estamos hablando de un dato personal, para ser más concretos y ligarlo con nuestro objeto de identificación, si un dato de geolocalización[74]

data, and repealing directive 95/46/EC (General Data Protection Regulation). En: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679. Consultado el 10 de diciembre de 2017.

[73] *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.*
https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=3E9B9352377E9603D6ABF4D87BBC0DA3.tplgfr24s_2?idArticle=LEGIARTI000006528061&cidTexte=LEGITEXT000006068624&dateTexte=20180101

[74] La geolocalización es la capacidad para obtener la ubicación geográfica real de un objeto, como un radar, un teléfono móvil o un ordenador conectado a Internet. La geolocalización puede referirse a la consulta de la ubicación, o bien para la consulta real de la ubicación. El término geolocalización está estrechamente relacionado con el uso de sistemas de posicionamiento, pero puede distinguirse de estos por un mayor énfasis en la determinación de una posición significativa (por ejemplo, una dirección de una calle) y no sólo por un conjunto de coordenadas geográficas. Este proceso es generalmente empleado por los sistemas de información geográfica, un conjunto organizado de hardware y software, más datos geográficos, que se encuentra diseñado especialmente para capturar, almacenar, manipular y analizar en todas sus posibles formas la información geográfica referenciada. En: https://es.wikipedia.org/wiki/Geolocalización consultado el 7 de octubre de 2017.

vive en un dispositivo electrónico, por ejemplo los datos de Waze[75] que viven en un iPhone[76], donde el usuario nunca se firmó o inscribió para utilizarlos, intentando hacer uso de éste de forma anónima, y de primera instancia podrían considerarse como anónimos, si éstos se correlacionan con todos aquellos datos que viven en el mismo dispositivo, es muy probable que podamos llegar a la identidad del usuario de dicho dispositivo, luego entonces los elementos de identidad de éste sujeto podrían vulnerarse.

Vale la pena únicamente esclarecer que deben de cumplirse diferentes criterios para que en verdad se considere que una persona pueda llegar a ser identificada, es cierto que las nuevas tecnologías permiten el relacionamiento de grandes volúmenes de información en tiempo récord, pero no todas las personas o empresas cuentan con el poder económico para llevar a cabo dicha actividad, por lo que siempre es importante llevar a cabo un análisis racional de posibilidad de que esto suceda o no.

Responsable: En términos del artículo 3 de la LIL, el responsable del tratamiento de un tratamiento de datos personales, a menos que lo designe expresamente la ley o el reglamento, es la persona, la autoridad pública, el departamento u organismo que determine sus fines y sus medios. Es decir que es aquella persona física o jurídica, de carácter público o privado, que decide sobre el tratamiento de los datos personales.

Tratamiento: El tratamiento es toda operación o conjunto de operaciones relacionadas con datos personales, sea cual sea el medio o proceso utilizado, para la recopilación, registro, organización, preservación, adaptación, modificación, extracción, consulta, uso, comunicación por transmisión de radiodifusión o cualquier otra forma de a disposición, conciliación o interconexión, bloqueo, eliminación o destrucción, de esta información.

[75] Waze es una aplicación social de tránsito automotor en tiempo real y navegación asistida por GPS desarrollada por Waze Mobile. Los usuarios de Waze son denominados Wazers, y, a diferencia de los softwares de navegación asistida por GPS tradicionales, este es mantenido por los usuarios y aprende de las rutas recorridas por sus usuarios para proveer información de enrutamiento y actualizaciones de tráfico en tiempo real. Las características que Waze ofrece incluyen: Búsqueda de destino por dirección completa, categoría, nombre del lugar, puntos de interés, o utilizando la información de los contactos, búsqueda integrada de destino: Google, Foursquare, Bing y Contactos, integración con redes sociales (Twitter y Facebook). En: https://es.wikipedia.org/wiki/Waze#cite_note-25 consultado el 26 de diciembre de 2017.
[76] iPhone es una línea de teléfonos inteligentes de alta gama diseñada y comercializada por Apple Inc. Ejecuta el sistema operativo móvil iOS, conocido hasta mediados de 2010 como "iPhone OS". En: https://es.wikipedia.org/wiki/IPhone consultado el 15 de diciembre de 2017.

El concepto anteriormente citado, extraído del artículo 2 de la propia Ley, es fruto de las diferentes reformas a la misma, ya que en un principio el tratamiento de datos personales que se encontraba regulado como tal, era el destinado a crear expedientes o archivos de usuarios, esta definición extendida de la LIL, comprende todo tipo de datos personales, inclusive aquellos que viajan o viven en la Internet, y por tanto le les directamente aplicable esta Ley.

Los tipos de tratamiento contemplados por la Ley, son: el tratamiento automatizado y el no automatizado, es importante aclarar que el simple hecho de que el manejo de cierto tipo de información sea llevado a cabo mediante una computadora, no conlleva de forma directa el tratamiento automatizado de datos personales, se tendría que analizar en un contexto global el tipo de herramientas informáticas, su operación, y la forma en que el algoritmo con el que fueron programadas manejan la información.

Expediente o archivo: Cabe señalar que la traducción a lengua española, del concepto original *fichier*, podría no concordar de manera precisa con lo que establece la LIL en su idioma original, la lengua española

Expediente	Archivo	Fichier
Del lat. expediens, -entis, part. act. de expedīre 'soltar', 'dar curso', 'convenir'. 2. m. Asunto o negocio que se sigue sin juicio contradictorio en los tribunales, a solicitud de un interesado o de oficio. 3. m. Conjunto de todos los papeles correspondientes a un asunto o negocio. U. señaladamente hablando de la serie ordenada de actuaciones administrativas,	Del lat. archīvum, y este del gr. ἀρχεῖον archeîon. 1. m. Conjunto ordenado de documentos que una persona, una sociedad, una institución, etc., producen en el ejercicio de sus funciones o actividades. 3. m. Acción y efecto de archivar (‖ guardar documentos en un archivo). Entregó la documentación para proceder a su archivo. 5. m. Inform. Conjunto de	[fiʃje] nom masculin 1. Collection, réunion de fiches. — Inform. Ensemble structuré d'informations; support de ces informations. 2. Meuble, boîte, classeur contenant des fiches.

y también de las judiciales en los actos de jurisdicción voluntaria.	datos almacenados en la memoria de una computadora que puede manejarse con una instrucción única.	

Por lo tanto, a lo largo de este trabajo utilizaremos la palabra archivo, la cual consideramos más precisa y acorde con la de la lengua francesa y que va en el mismo sentido que la LIL regula.

Los principios rectores de la Ley francesa, son principalmente cinco a diferencia de los ocho principios y diez deberes de la legislación mexicana. Sin embargo, en realidad los cinco pilares de la legislación francesa en materia de protección de datos personales, contemplan en la práctica, todas las obligaciones contenidas en la reglamentación mexicana, aunque quizás en menor detalle.

2.3.1 PRINCIPIO DE FINALIDAD

El principio de finalidad tal y como se contempla en la legislación francesa, en la base conceptual, no es muy diferente al que retomó la legislación mexicana, sin embargo, es cierto que de forma mucho más clara establece los límites de este principio y establece obligaciones precisas al respecto.

Básicamente, la finalidad consiste en determinar el objeto para el cual los datos están siendo recabados y para lo que el archivo generado va a servir. Dado que la legislación francesa obliga a la inscripción de dichos archivos ante la autoridad administrativa independiente, la Comisión Nacional de Informática y Libertades, es importante que desde un inicio las finalidades se establezcan de manera clara y precisa.

El artículo 6[77] de la Ley, prevé que las finalidades deben ser:

[77] Article 6 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Modifié par LOI n°2016-41 du 26 janvier 2016 - art. 193
Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :
1° Les données sont collectées et traitées de manière loyale et licite ;
2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des

a) Determinadas, explícitas y legítimas;

Los responsables deben claramente el objetivo de la creación de archivos que contengan datos personales, este objetivo debe ser acorde al objeto de la organización y además ser claro y comprensible.

b) Deben respetarse:

Los datos personales recabados para una cierta finalidad, no deben ser tratados posteriormente, para finalidades incompatibles con las originalmente declaradas y para las cuáles fueron recabados;

c) La finalidad debe permitir comprender la relevancia y pertinencia de los datos personales que se recaban.

En términos de la LIL, el principio de finalidad debe también permitir a los sujetos implicados en el tratamiento de datos, es decir, el titular, el responsable y a la autoridad, verificar si los datos recopilados son pertinentes o bien, no son los apropiados y estrictamente necesarios para lograr el propósito de la creación de ese archivo.

d) La finalidad permite delimitar los plazos de conservación de los datos personales.

El establecimiento de la finalidad en función del objetivo para el cual se colectaron los datos personales, éstos podrán ser conservados durante mayor o menor tiempo.

---

fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'au chapitre IX et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;
3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;
4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;
5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Es decir, que, en comparación con la legislación mexicana, el principio de finalidad y el de proporcionalidad se encuentran englobados en el primero, ya que también se basa en un criterio de minimización de la información tratada.

2.3.2 PRINCIPIO DE PERTINENCIA DE LA INFORMACIÓN

Toda información que se recabe y sobre la cual se vayan a generar archivos y por ende tratamiento, debe ser pertinente y estrictamente necesaria para cumplir el objetivo original del tratamiento.

Este principio también contempla que todos los datos que se recaben deben ser adecuados, pertinentes y no excesivos y en caso de ser inexactos o incompletos, establecer las medidas necesarias para la rectificación o eliminación de los mismos.

Aún y cuando esta obligación ya se menciona en el principio de finalidad, en este apartado mencionaremos algunos datos que por su naturaleza debe justificarse claramente su colecta y tratamiento.

Datos sensibles: Se entiende por dato sensible, toda información que revela orígenes raciales o étnicos, opiniones políticas, filosóficas o religiosas, afiliación sindical, salud o vida sexual de una persona. La Ley de Protección de Datos prohíbe la recopilación y el uso de estos datos, excepto en ciertos casos y en particular:

- Si el interesado ha dado su consentimiento expreso (activo, explícito y preferiblemente escrito, que debe ser libre, específico e informado),
- Si la persona interesada hace pública la información,
- Si son necesarios para salvaguardar la vida humana,
- Si su uso está justificado por el interés público y autorizado por la CNIL,
- Si se refieren a los miembros o adherentes de una asociación o una organización política, religiosa, filosófica, política o sindical.

Existe otro tipo de información que se considera restringida por Ley, por ejemplo, aquella relativa a los delitos, condenas y medidas de seguridad.

Esta información no se considera información confidencial, pero está estrictamente regulada por la ley.

Solo los tribunales, ciertas autoridades públicas y los auxiliares judiciales (abogados, por ejemplo) pueden tratarlos, así como a la víctima en el marco de la defensa de sus intereses.

El número de seguro social (NIR)[78]

El NIR o número de seguro social se asigna a cada persona en el momento del nacimiento sobre la base de los elementos de estado civil enviados por los ayuntamientos al INSEE[79]. Como es único para cada persona, particularmente identificador y significativo, su uso presenta un riesgo de registro de población y conciliaciones de archivos cada vez más importantes. Además, el uso de NIR está estrictamente regulado por la ley.

- Su uso se limita esencialmente a la esfera "salud-trabajo social"
- El uso de NIR siempre debe estar sujeto a una autorización previa de la CNIL)

2.3.3 LA CONSERVACIÓN DE LOS DATOS PERSONALES

Delimitar el tiempo de conservación de los datos personales es muy importante para garantizar al titular que no se está llevando a cabo el tratamiento de sus datos personales más allá de lo estrictamente necesario, incluyendo desde luego el tiempo necesario.

Los plazos de conservación de los datos deben fijarse en relación con la finalidad para los cuales fueron recabados los datos, de tal suerte que cuando la finalidad se extinga, estos sean debidamente suprimidos; sin embargo, existen otros plazos legales de conservación que también deben cumplirse o para los cuales hay referencia expresa en alguna Ley, por ejemplo, los registros laborales en Francia que tienen un plazo de conservación de 5 años, o el límite de un mes que tienen

[78] *Vérifier la pertinence des données*. En: https://www.cnil.fr/fr/verifier-la-pertinence-des-donnees consultado el 25 de noviembre de 2017.
[79] Institut National de la Statistique et des Études Économiques. En: https://www.insee.fr/fr/accueil consultado el 6 de enero de 2016.

todas la videograbaciones efectuadas con motivos de seguridad.

En el caso de la Ley francesa, sabe señalar que las omisiones a esta obligación son sancionadas por el Código Penal.

Algunos datos personales pueden, y en algunos casos, deben ser archivados cuando exista un interés legítimo.

La Ley reconoce 3 tipos de archivos:

- Las bases de datos activas,
- Archivos intermedios (acceso restringido, paso intermedio antes de la eliminación),
- Los archivos definitivos (datos de interés histórico, científico o estadístico que justifica que no se destruyan).

Cuando una Ley establece una obligación de conservación, la persona responsable del archivo debe asegurarse de que solo se archiven los datos relevantes para el cumplimiento de la obligación requerida o a efecto de hacer ejercer un derecho ante un tribunal. Por lo tanto, debe ordenar todos los datos recopilados para conservar solo los datos esenciales.

Los datos necesarios para cumplir una obligación legal o reglamentaria pueden archivarse durante el tiempo que sea necesario para cumplir con la obligación en cuestión. Los datos archivados se deben eliminar cuando el motivo que justifica su archivo se extinga.

Se deben implementar medidas técnicas, físicas y administrativas para proteger los datos archivados (destrucción, pérdida, alteración, diseminación o acceso no autorizado, etc.). Estas medidas deben garantizar un nivel de seguridad adecuado a los riesgos y la naturaleza de los datos.

Cuando el archivo sea almacenado por un contratista, el responsable debe asegurarse de que su proveedor de servicios cuenta con suficientes garantías con respecto a la seguridad y confidencialidad de los datos que se le han confiado.

En el caso de la información que ha sido suprimida de forma automatizada, el

responsable debe asegurarse de que efectivamente ya no existe en sus archivos, de lo contratrio podría hacerse acreedor a una sanción.

2.3.4 LOS DERECHOS DE LOS TITULARES

Los titulares de la información o sujetos interesados, deben disponer de un medio o mecanismo diseñado por el responsable para poder ejercer sus derechos y regular correctamente el uso de sus datos.

2.3.4.1 EL DERECHO A LA INFORMACIÓN

Para cumplir cabalmente con la ley y ser leales, la recopilación de datos personales debe ir acompañada de información clara y precisa de las personas sobre:

- La identidad del responsable;
- Finalidad o finalidades del tratamiento de los datos personales;
- Mencionar si la respuesta es obligatoria o facultativa, así como las consecuencias en caso de omisión de respuesta;
- El o los destinatarios de los datos y su calidad[80];
- La descripción clara de sus derechos (derecho de acceso, rectificación y oposición);
- Posibles transferencias de datos a países no pertenecientes a la UE.
- La puesta a disposición del aviso de privacidad para cumplir con el principio de información es preliminar a la recopilación de datos
- El soporte o formato del aviso dependerá de la forma en la que se recaben los datos personales.

La obtención del consentimiento

El consentimiento es derecho del titular de los datos personales, que debe ser, explícito y preferiblemente por escrito; a su vez, debe ser libre, específico e informado.

[80] En términos de la LIL, un destinatario de datos personales es toda persona autorizada para que le sean comunicados datos personales en razón de sus funciones.

El consentimiento es "previo" a la recopilación de datos.

La evidencia del consentimiento por parte del titular se requiere particularmente cuando:

- Se pretende recabar y tratar datos sensibles;
- Se presente llevar a cabo la reutilización de datos personales para fines distintos o complementarios a los anteriormente autorizados;
- Se requiere la autorización sobre el uso de cookies para ciertos propósitos;
- Cuando se pretende el uso de datos para fines de prospección comercial.

2.3.4.2 DERECHO DE ACCESO

Derecho de acceso directo: Toda persona física que justifique su identidad debidamente, tiene derecho a interrogar al responsable del tratamiento de sus datos personales[81], con la finalidad de que le sean comunicados a través de una forma accesible y comprensible los datos personales que le conciernen, así como toda información relacionada con el origen y obtención de los mismos.

El responsable del tratamiento de los datos, cuenta con un plazo de dos meses para responder a la solicitud que el interesado ha efectuado, pudiendo durante ese plazo solicitar a este último cualquier tipo de información suplementaria a fin de responder a su solicitud, en cuyo caso los plazos se suspenden hasta que la información solicitada sea completa, la suspensión de los plazos no aplica cuando el responsable efectúe una demanda de información abusiva, cualquier omisión de respuesta se entenderá como una negativa.

[81] Art. 39 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
I.-Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :
1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;
2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;
3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;
4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;
5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle.

Derecho de acceso indirecto: En los casos en los que el tratamiento se deba llevar a cabo por ministerio de Ley en pro de la seguridad nacional o seguridad del Estado, la información contenida en este tipo de archivos se considera confidencial y por lo tanto la solicitud de acceso no podrá hacerse de manera directa frente al responsable, sino que tendrá que efectuarse por parte del interesado ante la CNIL, ésta designará a un miembro que lleve a cabo las investigaciones necesarias y pertinentes que permitan, en su caso, la actualización, modificación o rectificación de la información del interesado, comunicándole que se ha llevado a cabo la actividad solicitud, sin informarle en ningún momento o darle acceso a los datos personales que viven en este tipo de archivos.

El derecho de acceso no es absoluto, es decir, el responsable puede negarse a brindarle información al titular respecto de sus datos personales en algunos casos, siempre y cuando justifique su negativa dentro del plazo de los dos meses señalados; se han reportado abusos en el ejercicio de este derecho por parte de ciertos titulares, que pretenden generar molestias a los responsables y en otros casos obtener información que no les corresponde, por ejemplo información de terceros que vive en el mismo archivo o documento al que desean tener acceso.

También opera la negativa o improcedencia, que debe ser debidamente notificada, cuando el responsable de datos personales no posea información alguna sobre el titular solicitante.

2.3.4.3 DERECHO DE RECTIFICACIÓN[82]

[82] Article 40 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
I. — Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.
Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.
En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.
Lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39.
Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa.
II. — Sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci.
En cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur cette demande dans un délai de trois

Toda persona física habiéndose identificado debidamente, tiene el derecho de exigir al responsable del tratamiento de sus datos personales, según el caso, que éstos sean rectificados, completados, actualizados, bloqueados o suprimidos en caso de que sean inexactos, incompletos, incorrectos o desactualizados; o bien, cuya recolección, uso, comunicación o conservación esté prohibida.

Cuando el interesado así lo solicite, el responsable deberá presentar pruebas, sin cargo para el solicitante, de que ha llevado a cabo las acciones requeridas según el párrafo anterior.

En caso de controversia, la carga de la prueba incumbe a la persona a cargo de la cual se ejerce el derecho de acceso, salvo cuando se compruebe que los datos controvertidos han sido comunicados por la persona interesada o con su consentimiento.

Si alguno de los datos del interesado ha sido transferido a un tercero, el responsable debe cumplir con las diligencias necesarias a efecto de notificar al titular las acciones llevadas a cabo conforme al primer párrafo.

A petición del interesado, el responsable del tratamiento debe eliminar lo antes posible los datos personales recopilados como parte de la oferta de servicios de la sociedad de la información cuando la persona interesada era menor al momento de la recolección. Cuando haya transmitido los datos en cuestión a un tercero responsable del procesamiento, tomará medidas razonables, incluidas las técnicas, teniendo en cuenta las tecnologías disponibles y los costos de implementación, para informar al tercero, de los datos que el interesado ha solicitado sean suprimidos, o bien la eliminación de cualquier enlace a ellos, o cualquier copia o reproducción de los mismos.

En caso de no ejecución de la eliminación de datos personales o en ausencia de una respuesta del responsable del tratamiento en el plazo de un mes desde la solicitud, el interesado puede remitir

---

semaines à compter de la date de réception de la réclamation.
Les deux premiers alinéas du présent II ne s'appliquent pas lorsque le traitement de données à caractère personnel est nécessaire :
1° Pour exercer le droit à la liberté d'expression et d'information ;
2° Pour respecter une obligation légale qui requiert le traitement de ces données ou pour exercer une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
3° Pour des motifs d'intérêt public dans le domaine de la santé publique ;
4° A des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit mentionné au présent II est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement ;
5° A la constatation, à l'exercice ou à la défense de droits en justice.

el asunto a la Comisión Nacional de Informática y Libertades, que decidirá sobre esta solicitud dentro de un período de tres semanas a partir de la fecha de recepción del reclamo.

Las excepciones al ejercicio del derecho de rectificación son las siguientes:

1 ° Ejercer el derecho a la libertad de expresión e información;

2 ° Para cumplir con una obligación legal que requiere el procesamiento de estos datos o para ejercer una misión de interés público o el ejercicio de la autoridad pública en su calidad de responsable;

3 ° Por razones de interés público en el campo de la salud pública;

4 ° Con fines de crear archivos de interés general, con fines de investigación científica o histórica o con fines estadísticos, en la medida en que el derecho mencionado en este artículo pueda hacer imposible o poner en grave peligro el logro de los objetivos del tratamiento mencionados;

5 ° El reconocimiento, ejercicio o defensa de los derechos en el tribunal.

Una importante innovación de la LIL, introducida en el año de 2016[83] en su artículo 40-1,

[83] Article 40-1 Modifié par LOI n°2016-1321 du 7 octobre 2016 - art. 63
I. - Les droits ouverts à la présente section s'éteignent au décès de leur titulaire. Toutefois, ils peuvent être provisoirement maintenus conformément aux II et III suivants.
II. - Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières.
Les directives générales concernent l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés.
Les références des directives générales et le tiers de confiance auprès duquel elles sont enregistrées sont inscrites dans un registre unique dont les modalités et l'accès sont fixés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.
Les directives particulières concernent les traitements de données à caractère personnel mentionnées par ces directives. Elles sont enregistrées auprès des responsables de traitement concernés. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation.
Les directives générales et particulières définissent la manière dont la personne entend que soient exercés, après son décès, les droits mentionnés à la présente section. Le respect de ces directives est sans préjudice des dispositions applicables aux archives publiques comportant des données à caractère personnel.
Lorsque les directives prévoient la communication de données qui comportent également des données à caractère personnel relatives à des tiers, cette communication s'effectue dans le respect de la présente loi.
La personne peut modifier ou révoquer ses directives à tout moment.
Les directives mentionnées au premier alinéa du présent II peuvent désigner une personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise

brinda la posibilidad a los titulares de datos personales de establecer pautas o instrucciones para el almacenamiento, el borrado y la comunicación de sus datos personales después de su muerte.

Estas pautas o instrucciones pueden ser generales o específicas.

Las pautas generales cubren todos los datos personales relacionados con el sujeto de datos y pueden registrarse con un tercero de confianza digital certificado por la Comisión Nacional de Informática y Libertades.

Las referencias de las instrucciones generales y del tercero de confianza con el que están registradas se inscriben en un único registro cuyas modalidades y acceso se fijan por decreto en el Consejo de Estado, tomado después de una opinión razonada y publicada de la Comisión Nacional del informática y libertades.

Las instrucciones específicas se refieren al procesamiento de los datos personales mencionados en estas directivas. Están registrados con los responsables de datos de que se trate. Están sujetos al consentimiento específico de la persona interesada y no pueden ser el resultado de la aprobación exclusiva por parte de esta última de las condiciones generales de uso.

Las instrucciones generales y específicas definen la manera en que la persona se propone ejercer, después de su muerte, los derechos mencionados en esta sección. El cumplimiento de estas

---

en œuvre aux responsables de traitement concernés. A défaut de désignation ou, sauf directive contraire, en cas de décès de la personne désignée, ses héritiers ont qualité pour prendre connaissance des directives au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés.
Toute clause contractuelle des conditions générales d'utilisation d'un traitement portant sur des données à caractère personnel limitant les prérogatives reconnues à la personne en vertu du présent article est réputée non écrite.
III. - En l'absence de directives ou de mention contraire dans lesdites directives, les héritiers de la personne concernée peuvent exercer après son décès les droits mentionnés à la présente section dans la mesure nécessaire :
- à l'organisation et au règlement de la succession du défunt. A ce titre, les héritiers peuvent accéder aux traitements de données à caractère personnel qui le concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession. Ils peuvent aussi recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers ;
- à la prise en compte, par les responsables de traitement, de son décès. A ce titre, les héritiers peuvent faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour.
Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en application du troisième alinéa du présent III.
Les désaccords entre héritiers sur l'exercice des droits prévus au présent III sont portés devant le tribunal de grande instance compétent.
IV. - Tout prestataire d'un service de communication au public en ligne informe l'utilisateur du sort des données qui le concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'il désigne.

pautas se entiende sin perjuicio de las disposiciones aplicables a los registros públicos que contienen datos personales.

Cuando las instrucciones prevean el suministro de datos que también incluyan datos personales relacionados con terceros, dicha comunicación se realizará de conformidad con esta Ley.

La persona puede cambiar o revocar sus instrucciones en cualquier momento. Las instrucciones también pueden designar a una persona responsable de su ejecución. Este último está facultado, en caso de muerte del titular, a tomar nota de las instrucciones y a solicitar su ejecución cara a los responsables de los datos personales del fallecido. En ausencia de una designación o, a menos que se indique lo contrario, en el caso de la muerte de la persona designada, sus herederos tienen derecho a conocer las citadas instrucciones y solicitar su implementación a los responsables involucrados.

Cualquier cláusula contractual en las condiciones generales para el uso del tratamiento de datos personales que limite las prerrogativas otorgadas a la persona bajo este artículo se considerará como no escrita.

En ausencia de instrucciones o de lo contrario especificado en dichas directivas, los herederos de la persona interesada pueden ejercer los derechos mencionados en esta sección después de su muerte en la medida necesaria:

- Para la organización y liquidación del patrimonio del difunto. Como tal, los herederos pueden acceder al procesamiento de los datos personales que le conciernen con el fin de identificar y obtener información útil para la liquidación y división del patrimonio. También pueden recibir comunicación de activos digitales o datos que se asemejan a recuerdos familiares, transmisibles a herederos;

- El hecho de que los responsables conozcan de la muerte del titular. Como tal, los herederos pueden proceder al cierre de las cuentas de los usuarios del fallecido, oponerse a la continuación del procesamiento de los datos personales que le conciernen o hacer que los actualicen.

Cuando así lo soliciten los herederos, el responsable deberá presentar prueba, sin cargo para el solicitante, de que ha llevado a cabo las operaciones requeridas de conformidad con el

párrafo anterior.

Los desacuerdos entre los herederos sobre el ejercicio de los derechos aquí previstos en se presentarán ante el tribunal de distrito competente.

Todo proveedor de un servicio de comunicación al público en línea informará al usuario del destino de sus datos, después de su muerte y le permitirá elegir si desea comunicar sus datos a un tercero que él designe.

2.3.4.4 DERECHO DE OPOSICIÓN[84]

El derecho de oposición de una persona al tratamiento de sus datos, forma parte de los principios fundamentales de protección de la vida privada y las libertades públicas. Sin embargo, este derecho no es un derecho absoluto, su ejercicio requiere que exista una justificación legítima a dicha oposición, dicha justificación legítima debe ser aportada por el titular y aplica siempre y cuando el tratamiento de los datos no sea motivado por una relación contractual en cumplimiento de una obligación legal o cuando haya disposición legal expresa.

Queda a salvo la oposición al tratamiento de datos personales para fines de prospección comercial.

2.3.5 LA SEGURIDAD DE LA INFORMACIÓN

Por último y no por ello menos importante, aparece la obligación relativa a la información de carácter personal.

El responsable está sujeto a cumplir con una obligación de seguridad[85]: debe tomar las

[84] Article 38 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.
Elle a le droit de s'opposer, sans frais, à ce que les données là concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.
Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement.

[85] Article 34 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

medidas necesarias para garantizar la seguridad de los datos que ha recopilado y para evitar su divulgación a terceros no autorizados.

El responsable debe identificar los riesgos para la vida privada de las personas que puedan resultar afectadas por el tratamiento de datos personales que efectuar o pretende efectuar, antes de determinar los medios apropiados para reducirlos. Para hacer esto, es necesario adoptar una visión global y estudiar las consecuencias para las personas involucradas.

El responsable debe tomar todas las precauciones necesarias, en vista de la naturaleza de los datos y los riesgos presentados por el procesamiento, para preservar la seguridad de los mismos y, en particular, para evitar que se distorsionen, dañen o que terceros tengan acceso no autorizado.

La CNIL propone un método compuesto por dos guías: el enfoque metodológico y las herramientas (modelos y ejemplos). Se complementan con una guía de buenas prácticas para enfrentar los riesgos.

Una propuesta de 4 pasos:

1. Estudio del contexto: Delimitar y describir los tratamientos considerados, su contexto y sus apuestas;

2. Estudio de las medidas: identificar las medidas existentes o planificadas (por un lado, para cumplir con los requisitos legales, por otro lado, para abordar los riesgos a la privacidad);

3. Evaluación de riesgos: evaluar los riesgos asociados con la seguridad de los datos que podrían tener un impacto en la privacidad de los interesados, a fin de verificar que sean tratados de manera proporcionada;

4. Validación: validar la forma en que se planea cumplir con los requisitos legales y tratar con los riesgos, o reiterar los pasos anteriores.

Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.

El catálogo de buenas prácticas ayuda a determinar medidas proporcionales a los riesgos identificados, actuando sobre:

- Los "elementos a proteger": minimizar los datos, cuantificar, anonimizar, permitir el ejercicio de los derechos.

- "Impactos potenciales": datos de respaldo, seguimiento de actividad, gestión de violaciones de datos.

- Las "fuentes de riesgo": controlar el acceso, gestionar a terceros, luchar contra códigos maliciosos.

- Los "soportes": reducen las vulnerabilidades de hardware, software, redes, documentos en papel.

Podemos concluir, que los principios rectores de la regulación francesa, son acordes a la directiva europea y como hemos visto, mucho de la legislación mexicana se inspira en el marco de protección de datos personales europeo.

La comparación de la legislación de protección de datos de la Unión Europea, México y los EE. UU. es una tarea difícil debido a las diferencias fundamentales estructurales, constitucionales y prácticas legales de cada uno de los países en comento. Ahora bien, nos enfocaremos en identificar las diferencias y deficiencias más importantes entre ellos.

La divergencia más prominente e importante se refiere a la protección constitucional de los datos personales. Si bien la protección de datos y la privacidad son derechos fundamentales en la Unión Europea y también son aplicables en el contexto del Cumplimiento de la Ley en Estados Unidos, no existe una protección equivalente entre estos.

Los antecedentes de la legislación europea y del reconocimiento de los derechos de Derechos de Privacidad y Protección de Datos, se han gestado desde la década de 1970 por jurisprudencia integral del Tribunal Europeo de Derechos Humanos y se ha ido desarrollando poco a poco en las últimas décadas a través de instrumentos importantes de la Unión Europea como

la Directiva 95/46 / CE, el Tratado de Funcionamiento de la Unión Europea y la Carta de los Derechos Fundamentales, así como la jurisprudencia de los tribunales de la Unión Europea. Los Estados Unidos, con sus restricciones a la protección de la Cuarta Enmienda, a través de la Doctrina de Terceros y la exclusión de personas no estadounidenses de la Cuarta Enmienda y la Protección de la Ley de Privacidad, siguen un enfoque muy diferente, que es contrario a la perspectiva y tradición de la Unión Europea en materia de privacidad y protección de datos como derechos fundamentales integrales.

El canon de protección de datos de la Unión Europea consta de varios principios, que se aplican independientemente del contexto. Incluyen, entre otros, normas sobre estándares de calidad de datos, sobre datos confidenciales, supervisión independiente e imparcial, el principio de limitación de las finalidades, reglas sobre intercambio interinstitucional de información o transferencia de datos a terceros, limitación a la temporalidad sobre el tratamiento de datos, revisión judicial efectiva y posibilidades de acceso, supervisión o verificación, elementos de proporcionalidad, requisitos de notificación después de posibles violaciones o vulneraciones a datos personales, derechos de acceso, rectificación y cancelación, así como normas sobre decisiones automatizadas y medidas de seguridad físicas, administrativas y técnicas.

Estos derechos y principios están sujetos a excepciones, sin embargo, están correctamente delimitadas y también son evaluadas bajo la lupa de los criterios de proporcionalidad debidos. Algunos de los derechos mencionados de la Unión Europea, como la notificación, supervisión o revisión judicial también se pueden encontrar en ciertas leyes de los Estados Unidos, por ejemplo, en la ECPA[86]. Sin embargo, solo existen en una forma mitigada y a menudo están sujetos a restricciones de gran alcance, cuando se trata del criterio de cumplimiento de la Ley o intereses de seguridad nacional. Estas restricciones no están limitadas por consideraciones de proporcionalidad, lo que lleva a una prevalencia estructural y regular del citado principio y los intereses de seguridad nacional.

Si bien algunos conceptos jurídicos son similares en cierta medida, la mayoría de las garantías de protección de datos de la Unión Europea simplemente no existen en la legislación estadounidense. Un ejemplo que ilustra un cierto grado de similitud es la supervisión. Si bien la idea de supervisión o vigilancia se puede encontrar en ambas jurisdicciones, la supervisión de acuerdo con las normas de la Unión Europea debe ser independiente, mientras que los mecanismos de supervisión

[86] *Electronic communications privacy Act of 1986 (ECPA)*. En: https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf consultada el 15 de enero de 2015.

interna dominan el criterio de aplicación de la ley de EE. UU. y el ámbito de seguridad nacional.

Otros principios básicos de protección de datos de la UE, como las restricciones sobre el uso posterior y la difusión de datos recopilados en un contexto de aplicación de la ley, la limitación de finalidades o los límites temporales al tratamiento de datos no existen o existen de manera rudimentaria en los EE. UU. En particular, el enfoque del intercambio de datos es fundamentalmente diferente. Si bien, en términos de la legislación de la Unión Europea, toda transferencia de datos a otras agencias interfiere con los derechos fundamentales y requiere una justificación específica, la mayoría de las veces, el intercambio de datos sin restricciones entre las autoridades locales, federales y la comunidad de inteligencia parece ser la regla y no la excepción en Estados Unidos.

Otra distinción crucial es el enfoque adoptado para determinar el alcance de una ley que proteja la privacidad y la protección de datos personales. Si bien las restricciones de privacidad en la Unión Europea generalmente se consideran en un equilibrio de intereses, centrándose en los requisitos de proporcionalidad, las leyes de los EE. UU. a menudo restringen el alcance de la aplicación de la ley misma, lo que hace considerablemente limitado su alcance desde el principio. Un ejemplo es el Proyecto de Ley de Reparación Judicial, cuya aplicación se limita a "registros cubiertos" y "países cubiertos".

Además, mientras que, en la Unión Europea, la existencia de un acto jurídico que interfiere en general con los derechos fundamentales es suficiente para que el individuo pueda interponer un recurso, la existencia de una recopilación masiva de datos en los EE. UU. no conlleva automáticamente un derecho individual de acción[87].

Otra diferencia importante se relaciona con las personas o sujetos tutelados, ya que mientras que, en la legislación de la Unión Europea, los derechos fundamentales cubren a todas las personas, así como las medidas de vigilancia, independientemente de su nacionalidad o domicilio, la legislación estadounidense distingue entre personas estadounidenses y no estadounidenses y discrimina a estas últimas. Esta distinción es claramente visible en las disposiciones que regulan la vigilancia de inteligencia extranjera, como la FISA y la Ley PATRIOTA. Las leyes recientemente introducidas,

[87] United States Court of Appeals, District of Columbia Circuit, Klayman v. Obama. En: https://assets.documentcloud.org/documents/2301510/read-the-dc-circuit-court-ruling-against-the-nsa.pdf consultado el 20 de diciembre de 2016.

como la Ley FREEDOM, no solucionan ni modifican esta situación. Solo en lo que respecta a las investigaciones penales ordinarias, los mismos derechos se aplican a las personas estadounidenses que a las personas no estadounidenses.

Sin embargo, la introducción de condiciones de acceso más estrictas para la recopilación de elementos tangibles y metadatos con fines de inteligencia extranjera a través del criterio recientemente introducido del término de selección específica en la Ley FREEDOM es una mejora en comparación con la recopilación de datos no regulada previamente. Su intención es limitar la recopilación masiva de datos mediante la introducción de criterios más restrictivos para identificar a una persona, entidad o cuenta específica durante la vigilancia ordenada.

Las autoridades gubernamentales ahora deben probar que buscan una persona o cuenta específica para obtener una orden FISA para acceder a metadatos, registros de detalles de llamadas u otras cosas tangibles. Lamentablemente, esta restricción recientemente introducida no se refiere al artículo 702 de la Ley de enmienda FISA, que autoriza la vigilancia de largo alcance de la información de inteligencia extranjera, incluidas las comunicaciones, el contenido, los metadatos u otros registros.

Con respecto a los acuerdos existentes de intercambio de datos entre la Unión Europea y EE. UU., como el régimen de puerto seguro[88], que demostró no ser suficiente ni aplicable a las normas actuales de protección de datos y tuvo que adaptarse para superar las deficiencias existentes, siendo sustituido por el "escudo de privacidad"[89].

En este orden de ideas, se puede deducir que incluso si todas las garantías de protección de datos existentes aplicables a los EE. UU. en el marco de aplicación de la ley y el marco de seguridad nacional fueran aplicables a los ciudadanos de la Unión Europea, habría una diferencia considerable en cuanto al nivel de privacidad y protección de datos personales.

CAPÍTULO III:

[88] Safe Harbor Agreement https://2016.export.gov/safeharbor/
[89] Privacy Shield https://www.privacyshield.gov/Program-Overview

LA IMPLEMENTACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES: EL ESTABLECIMIENTO DE ÓRGANOS ESPECIALES.

3.1 LOS ÓRGANOS DE PROTECCIÓN DE DATOS PERSONALES DE LOS ESTADOS UNIDOS DE AMERICA.

Como hemos visto anteriormente, uno de los grandes problemas del derecho norteamericano en materia de protección de datos personales es su legislación sectorial y poco precisa en ciertos aspectos, sin embargo, otro de los grandes problemas de fondo y aplicación de los que adolece es de una autoridad que específicamente regule y sancione los actos violatorios de la privacidad y a la protección de la información de carácter personal.

Sin embargo, de facto, la FTC, es decir la Federal Trade Comision, se ha convertido en la Autoridad de Protección de Datos (DPA) de facto de los Estados Unidos mediante el la aplicación agresiva y severa de la Sección 5 de la Ley de la FTC[90], que prohíbe las prácticas comerciales desleales o engañosas. La FTC ha cobrado a las empresas víctimas de infracciones de datos por prácticas comerciales injustas o engañosas sobre la base de que las infracciones fueron el resultado de que las empresas no adoptaron medidas de seguridad razonables. Las empresas a las que se dirige la FTC en estos casos cubren toda la gama, desde atención médica hasta hotelería, minoristas, redes sociales y otras compañías de Internet.

La FTC utiliza una variedad de herramientas para proteger la privacidad y la información personal de los consumidores. La principal herramienta de la FTC es implementar acciones de cumplimiento para detener las infracciones de la ley y exigir a las empresas que tomen medidas afirmativas para remediar el comportamiento ilícito. Esto incluye, cuando corresponda, la implementación de programas integrales de privacidad y seguridad, evaluaciones bienales de expertos independientes, reparación monetaria a los consumidores, devolución de ganancias adquiridas ilegalmente, eliminación de información de consumo obtenida ilegalmente y provisión de mecanismos robustos de transparencia y elección para los consumidores.

[90] Sección 5 de la Federal Trade Comision Act relativa a las prácticas desleales o engañosas. En: https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf. Consultado el 15 de enero de 2017.

Si una empresa viola una orden de la FTC, la FTC puede solicitar sanciones monetarias civiles por las violaciones. La FTC también puede obtener sanciones monetarias civiles por violaciones de ciertos estatutos y normas de privacidad, incluida la Ley de Protección de la Privacidad en Línea de los Niños, la Ley de Informes Crediticios y la Regla de Ventas de Telemercadeo.

Las otras herramientas de la FTC incluyen conducir estudios y emitir informes, organizar talleres públicos, desarrollar materiales educativos para consumidores y empresas, testificar ante el Congreso de los EE. UU. Y comentar propuestas legislativas y regulatorias que afectan la privacidad del consumidor y trabajar con socios internacionales en privacidad y responsabilidad global cuestiones.

En todo su trabajo de privacidad, los objetivos de la FTC se han mantenido constantes: proteger la información personal de los consumidores y garantizar que los consumidores tengan la confianza para aprovechar los numerosos beneficios que ofrece el mercado.

La FTC tiene una experiencia sinigual en la aplicación de reglas de privacidad del consumidor. Sus acciones de aplicación han abordado prácticas fuera de línea, en línea y en el entorno móvil. Ha traído acciones de cumplimiento contra compañías tan poderosas como Google, Facebook, Twitter y Microsoft. Las órdenes de cumplimiento de privacidad del consumidor de la FTC no solo protegen a los consumidores estadounidenses; más bien, protegen a los consumidores en todo el mundo de las prácticas desleales o engañosas de las empresas dentro de la jurisdicción de la FTC.

La FTC ha implementado acciones de cumplimiento dirigidas a una amplia gama de problemas de privacidad, que incluyen correo no deseado, redes sociales, publicidad dirigida basada en el comportamiento y hábitos del consumidor, spyware, intercambio de archivos punto a punto y dispositivos móviles. Estos asuntos incluyen más de 130 casos de spam y spyware y más de 40 demandas de privacidad generales. En 2016, la FTC anunció los siguientes casos de privacidad:

Según la FTC, hasta agosto de 2014, los operadores del sitio Ashley Madison

atrajeron a clientes, incluidos 19 millones de estadounidenses, con perfiles falsos de mujeres diseñados para convertirlos en miembros de pago. Los demandados aseguraron a los usuarios que su información personal era privada y estaba protegida de forma segura, pero, como se describe con más detalle a continuación, la FTC alegó que la seguridad de AshleyMadison.com era poco estricta.

Según la denuncia, la red de las empresas experimentó una importante violación de datos en julio de 2015, y en agosto de 2015, los piratas informáticos publicaron un perfil delicado, seguridad de la cuenta e información de facturación de más de 36 millones de usuarios de AshleyMadison.com. Supuestamente, esto incluía información que los demandados habían retenido sobre los usuarios que habían pagado 19 dólares por un servicio de *Eliminación total* para supuestamente eliminar sus datos del sitio.

La demanda acusaba, entre otras cosas, que los demandados tergiversaron que habían tomado medidas razonables para garantizar que AshleyMadison.com era segura, que habían recibido un "Premio de seguridad confiable" y que eliminarían toda la información de los consumidores que utilizaban su servicio de Eliminación Completa.

La demanda también acusaba a la empresa de tergiversar que las comunicaciones recibidas por los miembros eran de mujeres reales cuando en realidad eran de perfiles falsos. La FTC trabajó con una coalición de 13 estados y el Distrito de Columbia para asegurar un acuerdo, así como con la Oficina del Comisionado de Privacidad de Canadá y la Oficina del Comisionado de Información de Australia, quienes brindaron asistencia para la investigación de la FTC.

Desde 2002, la FTC ha presentado más de 60 casos contra compañías que han incurrido en prácticas desleales o engañosas que ponen los datos personales de los consumidores en un riesgo grave.

Además de las acusaciones por violaciones a la privacidad descritas anteriormente, los operadores del sitio de citas Ashley Madison con sede en Toronto acordaron liquidar las multas de la FTC y aceptar los cargos estatales que prueban engañaron a los consumidores y no protegieron la información de cuenta y perfiles de 36 millones de usuarios en julio de

2015.

El sitio cuenta con miembros de más de 46 países. Según la demanda, le empresa no tenía una política escrita de seguridad de la información, controles de acceso razonables, capacitación de seguridad adecuada para los empleados, no tenían conocimiento de si los proveedores de servicios de terceros usaban medidas de seguridad razonables y no tenían medidas para monitorear la efectividad de su sistema.

Parte del acuerdo final requiere que los demandados implementen un programa integral de seguridad de datos, que incluye evaluaciones de terceros. Además, los operadores acordaron pagar un total de $1.6 millones de dólares para liquidar la multa de la FTC y las acciones estatales correspondientes[91].

En términos de lo señalado expresamente por el Congreso, la FTC tiene autoridad para desarrollar reglas aplicables a áreas específicas de privacidad y seguridad del consumidor. Desde 2000, la FTC ha promulgado reglas en varias de estas áreas:

- La Regla de Notificación de Violación de Salud[92] requiere que ciertos negocios basados en Web notifiquen a los consumidores cuando se viola la seguridad de su información electrónica de salud.

- La regla de las banderas rojas[93] exige que las instituciones financieras y ciertos acreedores tengan programas de prevención de robo de identidad para identificar, detectar y responder a patrones, prácticas o actividades específicas que puedan indicar el robo de identidad o algún tipo de fraude relacionado.

[91] FTC Earns Prestigious International Award for AshleyMadison.com Data Breach Investigation Shares honor with privacy law authorities in Australia and Canada. En: https://www.ftc.gov/news-events/press-releases/2017/09/ftc-earns-prestigious-international-award-ashleymadisoncom-data consultado el 30 de septiembre de 2017.
[92] Health Breach Notification Rule. En: https://www.ftc.gov/tips-advice/business-center/guidance/health-breach-notification-rule consultado el 20 de agosto de 2016.
[93] Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, as Amended by the Red Flag Program Clarification Act of 2010. En: Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, as Amended by the Red Flag Program Clarification Act of 2010. Consultado el 6 de enero de 2016.

- La regla COPPA[94] Children's Online Privacy Protection Rule, requiere que los sitios web y aplicaciones obtengan el consentimiento de los padres antes de recabar información personal de niños menores de 13 años. La regla fue revisada en 2013 para fortalecer la protección de privacidad de los niños y les da a los padres mayor control debajo de 13.

- La Regla de Privacidad de GLB[95] (Gramm-Leach-Bliley Act), establece cuándo los concesionarios de automóviles deben proporcionar al consumidor un aviso que explique las políticas y prácticas de privacidad de la institución y brinde al consumidor la oportunidad de optar por no divulgar cierta información a terceros no afiliados.

- La Regla de Garantías GLB[96] requiere que las instituciones financieras sobre las cuales la FTC tiene jurisdicción, para desarrollar, implementar y mantener un programa integral de seguridad de la información que contenga medidas administrativas, técnicas y físicas que salvaguaren correctamente la información. En 2016, la FTC solicitó comentarios públicos sobre la Regla como parte de su revisión sistémica de todas las reglas y guías actuales de la FTC.

- La Regla de Ventas de Telemarking[97] requiere que los agentes de telemercadeo hagan revelaciones específicas de información material; prohíbe tergiversaciones de información y hechos; limita las horas que los agentes de telemercadeo puedan llamar a los consumidores; y establece restricciones de pago para la venta de ciertos bienes y servicios. Las disposiciones de la Regla de No Llamar, prohíben a los vendedores y

[94] Children's Online Privacy Protection Rule. En: https://www.gpo.gov/fdsys/pkg/FR-2013-01-17/pdf/2012-31341.pdf consultado el 20 de marzo de 2016.
[95] Privacy of Consumer Financial Information. En: https://www.gpo.gov/fdsys/pkg/FR-2000-05-24/pdf/00-12755.pdf consultado el 20 de marzo de 2016.
[96] Standards for Safeguarding Customer Information; Final Rule. En: https://www.gpo.gov/fdsys/pkg/FR-2002-05-23/pdf/02-12952.pdf consultado el 20 de marzo de 2016.
[97] Telemarketing Sales Rule; Final Rule. En: https://www.gpo.gov/fdsys/pkg/FR-2003-01-29/pdf/03-1811.pdf consultado el 20 de marzo de 2016.

agentes de telemercadeo incurrir en ciertas prácticas abusivas que infringen el derecho del consumidor a no ser molestado o ser dejado solo, incluida la llamada a una persona cuyo número figura en el Registro No Llamar o que ha solicitado no recibir llamadas de *telemarking* de alguna compañía en particular. La Regla también prohíbe las llamadas automáticas (llamadas de telemercadeo comercial pregrabadas a los consumidores) a menos que el teleoperador haya obtenido permiso por escrito de los consumidores que desean recibir dichas llamadas. La Regla fue revisada en 2016 para prohibir cuatro tipos discretos de métodos de pago favorecidos por estafadores.

- La regla de *Controlling the Assault of No Solicited Pornography and Marketing* (CAN-SPAM)[98] está diseñada para proteger a los consumidores del correo electrónico comercial engañoso y requiere que las empresas tengan mecanismos de exclusión.

- La Regla de eliminación según la Ley de Transacciones de Crédito Justas y Precisas de 2003 ("FACTA")[99], que modificó la FCRA, requiere que las empresas eliminen los informes crediticios y la información derivada de ellos de manera segura. En 2016, la FTC solicitó comentarios públicos sobre la Regla de eliminación como parte de su revisión sistémica de todas las reglas y guías actuales de la FTC. Entre otras cosas, la Comisión solicitó comentarios sobre si la definición de "información del consumidor" debería ampliarse para incluir información agregada o información que pueda vincularse razonablemente con un individuo.

- La regla de exclusión previa a la pantalla bajo FACTA[100] requiere que las compañías que envían solicitudes de crédito o seguros "pre-autorizadas" a

[98] Controlling the Assault of No Solicited Pornography and Marketing CAN-SPAM. En: https://www.ecfr.gov/cgi-bin/text-idx?SID=9bfc83ad4923395cbf9d824ae3cef81b&mc=true&node=pt16.1.316&rgn=div5 consultado el 25 de marzo de 2016.
[99] Disposal of Consumer Report Information and Records; Final Rule. En: https://www.gpo.gov/fdsys/pkg/FR-2004-11-24/pdf/04-25937.pdf consultado el 20 de diciembre de 2016.

[100] Prescreen Opt-Out Disclosure; Final Rule. En https://www.gpo.gov/fdsys/pkg/FR-2005-01-31/pdf/05-1678.pdf consultado el 20 de diciembre de 2016.

los consumidores, proporcionen avisos simples y fáciles de entender que expliquen el derecho de los consumidores a optar por no recibir futuras ofertas.

En conclusión, en Estados Unidos, la FTC, es la que se ha encargado de la aplicación de las reglas de privacidad en diferentes ámbitos de la industria en el ámbito comercial.

3.2 EL INAI

En México, el derecho a la información es fundamental, expresado en el artículo sexto de la Constitución mexicana; con la alternancia en el poder, se generaron espacios de participación ciudadana, lo que permitió exigir que las acciones gubernamentales transparentaran el uso de los recursos públicos. El 11 de junio del 2002 se firmó el decreto de promulgación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, del que se derivó la creación del Instituto Federal de Acceso a la Información (IFAI).

La historia del IFAI, su naturaleza jurídica, atribuciones y diseño institucional, están inexorablemente ligados a las circunstancias que rodearon la creación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en México. Cabe por ello recordar que, en su diseño original, esa Ley estaba concebida para ser aplicada exclusivamente en el ámbito de la administración pública federal.

Fue durante su proceso de discusión y negociación que se determinó ampliar su ámbito de aplicación para incluir a todos los poderes federales y los organismos constitucionales autónomos. Sin embargo, fue también durante ese proceso que se acordó establecer y diseñar con detalle un órgano administrativo, dotado de autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho de acceso a la información, de supervisar la aplicación de la ley y de resolver las controversias que se suscitaran entre los particulares y la administración pública federal respecto de las solicitudes de acceso a la información y de protección de acceso y rectificación datos personales.

A esta función se le fueron añadiendo otras, que le dieron una naturaleza peculiar al IFAI. En efecto, sus atribuciones van mucho más allá de la mera resolución de controversias, pues de acuerdo con la Ley, le corresponde ser el órgano regulador en materia de información y protección de datos personales para la administración pública federal; la de supervisar el cumplimiento de la ley; la de promover el ejercicio del derecho de acceso a la información entre los ciudadanos, y la de generar una nueva cultura del manejo de la información, tanto entre los servidores públicos como entre los ciudadanos.

El IFAI se constituyó formalmente, mediante decreto presidencial publicado en el Diario Oficial de la Federación el 24 de diciembre de 2002, como un organismo descentralizado, no sectorizado, con personalidad jurídica y patrimonio propio. Para efecto de garantizar su autonomía presupuestaria y administrativa se le considera como una entidad paraestatal de control indirecto no apoyada presupuestalmente. Adicionalmente, se precisa que el órgano interno de control no puede interferir en las decisiones sustantivas del Instituto[101].

El 7 de febrero de 2014, se publicó en el Diario Oficial de la Federación, el Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, por medio del cual se amplían los sujetos obligados frente a los cuales se ejercer el derecho de acceso a la información pública, se sientan las bases para articular un Sistema Nacional de Transparencia, y se brinda autonomía constitucional a los órganos garantes federal y estatales, ampliando sus facultades y competencia.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es el organismo constitucional autónomo garante del cumplimiento de dos derechos fundamentales: el de acceso a la información pública y el de protección de datos personales.

Para el primero, garantiza que cualquier autoridad en el ámbito federal, órganos autónomos, partidos políticos, fideicomisos, fondos públicos y sindicato; o cualquier persona

[101] El futuro del ifai: consideraciones sobre su autonomía constitucional. En: https://archivos.juridicas.unam.mx/www/bjv/libros/7/3196/2.pdf consultado el 14 de mayo de 2016.

física, moral que reciba y ejerza recursos públicos o realice actos de autoridad te entregue la información pública que solicites.

Para el segundo, garantiza el uso adecuado de los datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición que toda persona tiene con respecto a su información.

Cuenta con cuatro objetivos primordiales:

Objetivo 1: Garantizar el óptimo cumplimiento de los derechos de acceso a la información pública y la protección de datos personales.

Objetivo 2: Promover el pleno ejercicio de los derechos de acceso a la información pública y de protección de datos personales, así como la transparencia y apertura de las instituciones públicas.

Objetivo 3: Coordinar el Sistema Nacional de Transparencia y de Protección de Datos Personales, para que los órganos garantes establezcan, apliquen y evalúen acciones de acceso a la información pública, protección y debido tratamiento de datos personales.

Objetivo 4: Impulsar el desempeño organizacional y promover un modelo institucional de servicio público orientado a resultados con un enfoque de derechos humanos y perspectiva de género.

Específicamente en materia de protección de datos personales y con fundamento en la Ley, el Instituto tiene las siguientes facultades y atribuciones.

> *"Artículo 38.- El Instituto, para efectos de esta Ley, tendrá por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particular aquellas relacionadas con el*

cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento.

Artículo 39.- El Instituto tiene las siguientes atribuciones:

I. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación;

II. Interpretar en el ámbito administrativo la presente Ley;

III. Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley;

IV. Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables de esta Ley, para efectos de su funcionamiento y operación;

V. Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable;

VI. Conocer y resolver los procedimientos de protección de derechos y de verificación

señalados en esta Ley e imponer las sanciones según corresponda;

VII. Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos;

VIII. Rendir al Congreso de la Unión un informe anual de sus actividades;

IX. Acudir a foros internacionales en el ámbito de la presente Ley;

X. Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes;

XI. Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en Posesión de los Particulares y brindar capacitación a los sujetos obligados, y

XII. Las demás que le confieran esta Ley y demás ordenamientos aplicables."

Cabe destacar que la legislación mexicana, prevé que distintas autoridades en su carácter de reguladoras, mantengan ciertas atribuciones y facultades en el ámbito de sus actividades, por ejemplo: la Secretaría de Salud, es la dependencia del Poder Ejecutivo que

se encarga primordialmente de la prevención de enfermedades y promoción de la salud de la población; dentro de la citadas obligaciones seguirá siendo competente para regular y en su caso, sancionar aquellas conductas ilícitas en materia de protección de datos personales en el ámbito de salud.

"Artículo 40.- La presente Ley constituirá el marco normativo que las dependencias deberán observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda, con la coadyuvancia del Instituto.

Artículo 41.- La Secretaría, para efectos de esta Ley, tendrá como función difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano; promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto.

Artículo 42.- En lo referente a las bases de datos de comercio, la regulación que emita la Secretaría, únicamente será aplicable a aquellas bases de datos automatizadas o que formen parte de un proceso de automatización.

Artículo 43.- La Secretaría tiene las siguientes atribuciones:

I. Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial;

II. Fomentar las buenas prácticas comerciales en materia de protección de datos personales;

III. Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad en coadyuvancia con el Instituto, a que se refiere la presente Ley;

IV. Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general a que se refiere el artículo 40, en coadyuvancia con el Instituto;

V. Fijar los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere el artículo 44 de la presente Ley, incluido la promoción de Normas Mexicanas o Normas Oficiales Mexicanas, en coadyuvancia con el Instituto;

VI. Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento;

VII. Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales;

VIII. Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales;

IX. Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial, y

X. Apoyar la realización de eventos, que contribuyan a la difusión de la protección de los datos personales.

Artículo 44.- Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la presente Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento.

Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares. Dichos esquemas serán notificados de manera simultánea a las autoridades sectoriales correspondientes y al Instituto.

3.3 LA CNIL

Para asegurar la puesta en marcha de la Ley de Informática y Libertades de 197, se instauró un organismo especializado: La Comisión Nacional de Informática y Libertades (CNIL). En sus orígenes, la CNIL estaba encargada de vigilar y asegurar el respeto de las disposiciones de la citada Ley, y en particular informar a los sujetos implicados, sus derechos y obligaciones. La Comisión dispone de un poder reglamentario en los casos previstos en la propia Ley.

Cabe recordar, que la Ley, tal y como fue concebida originalmente, tuvo que reformarse para poder trasponer la Directiva Europea de 1995 (95/46/CE), a la legislación francesa, por lo tanto, fue reformada en el año de 2004, y con esta reforma también evolucionaron las atribuciones y facultades de la CNIL, ya que mientras la redacción original, se enfocaba en los procedimientos de requisitos previos para autorizar el procesamiento por

parte de la CNIL, la nueva redacción instaura un catálogo de controles y sanciones.

En este sentido, las atribuciones de la CNIL, pasan de ser una serie de controles aplicables *a priori*, a convertirse en un control *a posteriori*. Este tipo de controles, pretende lograr su objetivo de ejercer su poder sancionador en varias etapas.

Una vez que la CNIL, después de haber constatado un incumplimiento de las obligaciones contenidas en la Ley, puede apercibir al responsable del tratamiento para que este subsane dicho incumplimiento; si el responsable hace caso omiso y no pone en marcha las medidas necesarias para estar en regla, la CNIL puede imponer una sanción pecuniaria o incluso impedir o cesar el tratamiento de los datos, en función de la gravedad de la amenaza y lo que represente para los derechos y libertades de los titulares de la información.

La CNIL apoya a los profesionales en su cumplimiento y ayuda a las personas a controlar sus datos personales y ejercer sus derechos. Analiza el impacto de las innovaciones tecnológicas y los usos emergentes en la privacidad y las libertades. Además de ello, trabaja estrechamente con sus contrapartes europeas e internacionales para desarrollar una regulación armonizada.

Cuenta con 4 misiones principales:

1. Informar y proteger:

El CNIL informa a personas y profesionales y responde a sus solicitudes. Les proporciona herramientas prácticas y pedagógicas e interviene regularmente para motivar y organizar las acciones de formación y sensibilización en el tema, especialmente en el contexto de la educación digital.

Su misión es promover el uso de tecnologías de privacidad, incluidas las tecnologías de encriptación de datos.

2. Acompañar y aconsejar

La regulación en materia de protección de datos personales pasa por diferentes instrumentos, todos ellos tienen el objetivo de hacer que las organizaciones cumplan cabalmente con sus obligaciones. Por ejemplo, se emiten opiniones sobre proyectos de leyes o decretos, autorización para los tratamientos de datos sensibles, recomendaciones que establecen una postura doctrinal, también se crean y promueven marcos legales que simplifican las formalidades preliminares, y se da respuesta a solicitudes de asesoramiento.

La CNIL también ofrece una caja de herramientas a las organizaciones que deseen avanzar en su proceso de cumplimiento: en su calidad de corresponsales de informática y libertades (CIL), etiquetas, paquetes de cumplimiento (normas de referencia sectoriales), BCR (Reglas Corporativas Vinculantes) que enmarcan las transferencias de datos personales a multinacionales fuera de la Unión Europea.

Certifica el cumplimiento de los procesos de anonimización de los datos personales con el fin de que sean puestos en línea y reutilizados.

3. Control y sanción

Las visitas de inspección en sitio, en el lugar, auditoría o en línea permite a la CNIL verificar la implementación concreta de la ley. Además, se elabora un programa de controles de acuerdo con los temas actuales, los principales problemas identificados y las quejas presentadas a la CNIL.

La CNIL es competente para controlar los sistemas de video vigilancia autorizados por las prefecturas.

Durante una inspección en sitio, el CNIL cuenta con facultades expresas para solicitar:

- Acceso a todos los locales comerciales,
- Solicitar y hacer copias de los documentos que consideres necesarios,
- Reúna información útil y solicite declaraciones de los responsables,

- Acceder a los programas y datos de la computadora,

Después de los controles de auditoría efectuados, y dependiendo de las inconformidades encontradas, el presidente de la CNIL puede decidir las acciones formales a tomar, ya que podrían ser implemente una serie de apercibimientos que obliguen al responsable a subsanar sus faltas.

El comité ejecutivo de la CNIL, compuesto por 5 miembros y un presidente, distinto del presidente de la CNIL, puede pronunciar diversos tipos de sanciones después de haber llevado a cabo el procedimiento legal pertinente: por ejemplo, una multa financiera (excepto para el Estado), que puede ser de hasta 3 millones de euros. Esta sanción puede hacerse pública; el comité ejecutivo, también puede ordenar la comunicación de su decisión a la prensa u ordenar que los organismos sancionados informen individualmente a las personas afectadas a expensas del sancionado. El monto de las multas es recaudado por el Tesoro Público y no por la CNIL.

El comité ejecutivo de la CNIL también puede pronunciar:

- Una orden judicial para detener el tratamiento.
- Una revocación de la autorización otorgada por la CNIL.
- En caso de una violación grave e inmediata de los derechos y libertades de los titulares, el presidente de la CNIL puede solicitar la aplicación de medidas cautelares, a la jurisdicción competente. También puede informar al Ministerio Público de cualquier violación de la ley de la que tenga conocimiento.

4. Anticipar

Como parte de su actividad de innovación y previsión, la CNIL establece una línea de tiempo para detectar y analizar tecnologías o nuevos usos que pueden tener un impacto significativo en la privacidad. Tiene un laboratorio que le permite experimentar con productos o aplicaciones innovadores. Contribuye al desarrollo de soluciones tecnológicas

que protegen la privacidad al asesorar a las empresas lo correctamente posible, para que sean capaces de diseñar sus procesos bajo una estructura de privacidad por diseño (*privacy by design*), tal y como lo hacen en el modelo norteamericano.

Para reforzar sus criterios, ha creado un Comité de prospectiva que convoca a expertos externos para que lo asesoren en un programa anual de estudios y exploraciones. Su misión es conducir una reflexión sobre cuestiones éticas y cuestiones sociales planteadas por la evolución de las tecnologías digitales.

CAPÍTULO IV

SANCIONES E INFRACCIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Las sanciones aplicadas por cada una de las autoridades mencionadas en el capítulo anterior, son variables en función de diversos criterios, sin embargo, en los tres casos pueden considerarse como sanciones altas, financieramente hablando, con independencia del posible daño en la reputación de las empresas infractores, ya que, en las tres distintas jurisdicciones, las infracciones suelen ser de interés público y por lo tanto la prensa puede conocer de ellas y difundirlas.

Una gran e interesante diferencia es que tanto en el caso de México como en el de Francia, es la tesorería nacional quien recibe el importe de las multas, con independencia de las eventuales indemnizaciones que puedan solicitarse por el titular vía civil, después de seguirse los procesos judiciales correspondientes. En Estados Unidos, la FTC, cuenta con acuerdos de cooperación con diferentes instancias civiles y criminales, que permiten formular casos exitosos en contra de los infractores.

La Comisión se enfoca en su programa de cumplimiento de órdenes, que puede ser complementada con otro tipo de litigios. El programa incluye acciones de desacato civil, el programa de enlace criminal y procedimientos de cobro para obtener el pago de las sentencias. Por lo tanto, la FTC puede gestionar los reembolsos de manera directa a los afectados, situación altamente benéfica para los ciudadanos norteamericanos.

Algunas de las cifras de la FTC del año 2016 se muestran a continuación:

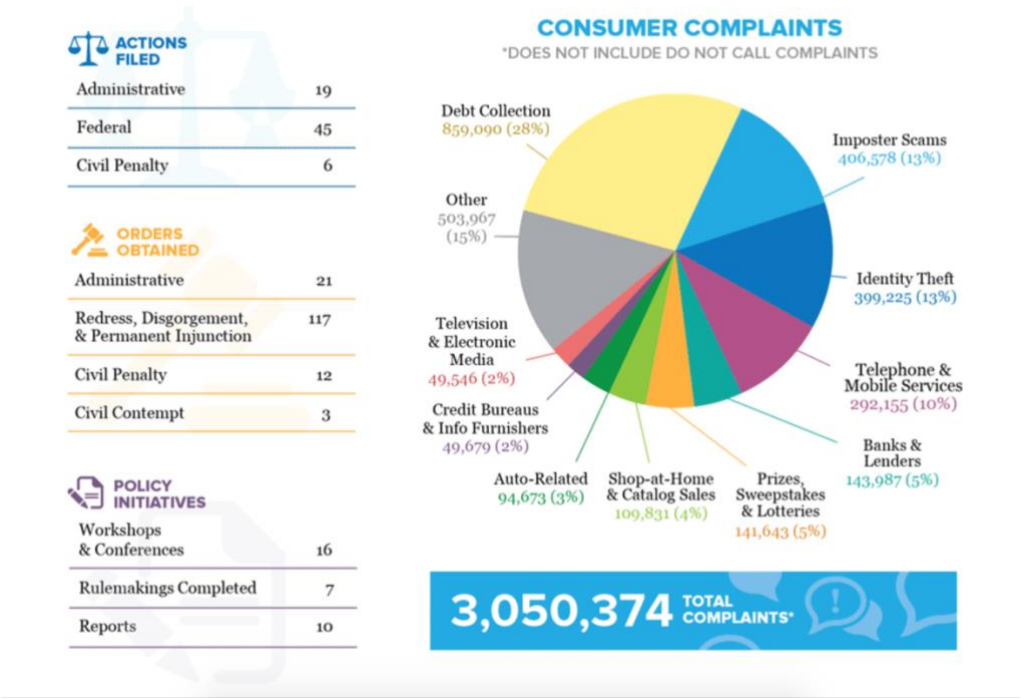


Fig. 7 Estadística del número de quejas atendidas por la FTC en 2016, clasificadas por sector y actividades.[102]

[102] Disponible en: https://www.ftc.gov/node/1205233 consultado el 15 de julio de 2017.

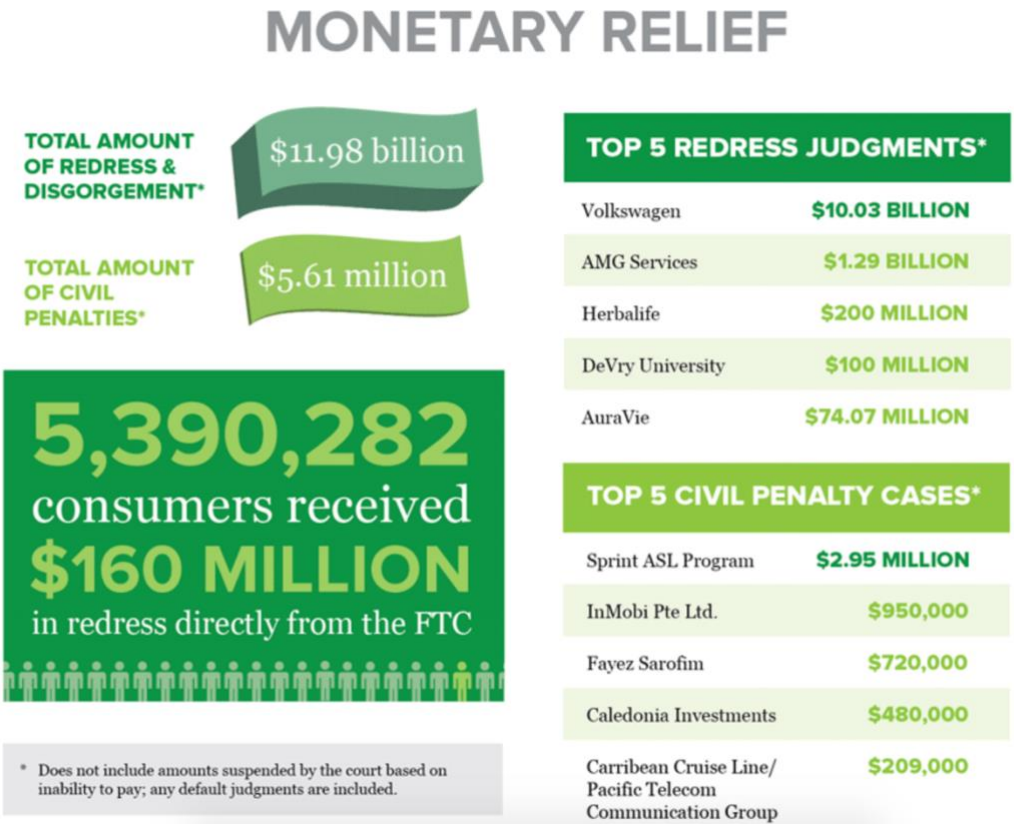


Fig. 8 Estadística de compensaciones económicas obtenidas por la FTC en 2016 luego de las sanciones impuestas a las referidas empresas[103].

En el caso de las sanciones impuestas por el INAI, las sanciones que están comprendidas en la Ley (LFPDPPP), son las siguientes:

> *"Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:*
>
> *I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada,*

[103] Idem

en los términos previstos en esta Ley;

II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;

III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;

IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;

V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;

VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;

VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;

VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;

IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo

dispuesto por el artículo 12;

X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;

XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;

XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;

XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;

XIV. Obstruir los actos de verificación de la autoridad;

XV. Recabar datos en forma engañosa y fraudulenta;

XVI. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;

XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;

XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley, y

XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.

Artículo 64.- Las infracciones a la presente Ley serán sancionadas por el Instituto con:

I. El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en la fracción I del artículo anterior;

II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior;

III. Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior, y

IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Artículo 65.- El Instituto fundará y motivará sus resoluciones, considerando:

I. La naturaleza del dato;

II. La notoria improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular, en términos de esta Ley;

III. El carácter intencional o no, de la acción u omisión constitutiva de la infracción;

IV. La capacidad económica del responsable, y

V. La reincidencia.

Artículo 66.- Las sanciones que se señalan en este Capítulo se impondrán sin perjuicio de la responsabilidad civil o penal que resulte."

La Ley contempla incluso, tres tipos penales, por lo que, si la conducta del infractor se encuadra en cualquiera de éstos, podrá incluso tener una pena corporal o de prisión. Las conductas que pueden llegar a ser constitutivas de un delito, se detallan a continuación:

"Artículo 67.- Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

Artículo 68.- Se sancionará con prisión de seis

meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.

Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

En cifras publicadas a través de un comunicado del propio INAI, en el primer semestre de 2016, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales instauró 30 Procedimientos de Imposición de Sanciones en contra de empresas y/o personas físicas que infringieron la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

De enero a junio de ese año, el Instituto impuso 22 sanciones económicas, cuyos montos suman 50 millones 611 mil 145 pesos; los tres sectores con el mayor número de multas son el de servicios financieros y de seguros, el de información en medios masivos y el de servicios educativos.

De la entrada en vigor de la LFPDPPP, en enero de 2012, a junio de 2016, el monto total de las multas impuestas por el INAI fue de 235 millones 669 mil 887 pesos.

Las infracciones cometidas con mayor frecuencia y por las cuales las empresas o personas físicas se han hecho acreedoras a una sanción económica son: tratar datos personales en contravención a los principios establecidos en la Ley (licitud, información, responsabilidad, lealtad y consentimiento); recabar o transferir datos personales sin el consentimiento expreso de las personas, y omitir el Aviso de Privacidad, alguno o todos los elementos previstos en la norma.

Los Procedimientos de Imposición de Sanciones se inician por la conclusión de los procedimientos de protección de derechos o de verificación cuyas resoluciones así lo ordenen.

Al 30 de junio de este año, se han presentado 185 solicitudes de protección de derechos ARCO (Acceso, Rectificación; Cancelación y Oposición); cabe señalar que en una solicitud pueden ejercerse uno o más de estos derechos.

Asimismo, el Instituto ha recibido 232 denuncias en materia de protección de datos; en 165 casos inició un expediente de investigación preliminar, de los cuales 77 ya fueron concluidos y 88 se encuentran en trámite.

Por otro lado, el INAI ha iniciado 49 Procedimientos de Verificación, a fin de verificar el cumplimiento de la Ley y la normatividad derivada; de ese total, 23 fueron concluidos y 26 están en trámite.

Los cinco sectores con el mayor número de verificaciones son el de servicios financieros y de seguros, con 15 procedimientos; el de información en medios masivos y servicios educativos, con 5 cada uno, y el de servicios de apoyo a los negocios y otros servicios, con 4 cada uno.

El estatus *quo* de la CNIL en el año 2016 revela lo siguiente:

En 2016, la CNIL llevó a cabo 430 inspecciones *in situ*, por requerimiento, sobre documentación e inspecciones en línea. Prácticamente 300 controles se llevaron a cabo en sitio, por un centenar de controles en línea. Las auditorías sobre documentos y bajo requerimiento, particularmente adaptadas a organizaciones establecidas fuera de Francia, representaron alrededor de 30 misiones.

La combinación de diferentes modos de intervención se ha implementado con éxito en muchas misiones que han detectado incumplimientos en materia de protección de datos ("brechas de seguridad" o "filtraciones de datos"): después de un control efectuado en línea, y habiendo fijado las pruebas de omisiones, los agentes autorizados viajan a la organización interesada para buscar hallazgos adicionales. Una veintena de estas operaciones se llevaron a cabo en 2016, que ya han resultado en cuatro apercibimientos, uno de ellos público.

El 20% de los controles se refería a dispositivos de videovigilancia instalados en lugares abiertos al público, sujetos al código de seguridad interno. Las irregularidades más frecuentemente observadas se relacionan con:

- Falta de autorización o autorización caducada de la prefectura;
- Información poco clara o faltante al público;
- Poca seguridad aplicada a los soportes donde se almacenan los datos, y facilidad de acceso no autorizado.
- Los organismos auditados, en particular las autoridades locales, con mayor frecuencia han puesto sus dispositivos en conformidad después de los hallazgos de la CNIL.

El 20% de los controles sobre el tratamiento de datos personales se llevaron a cabo en el marco de los temas planificados en el programa anual 2016:

SNIIRAM: La CNIL ha llevado a cabo una docena de controles en el sistema nacional de información de seguros de salud (SNIIRAM), una de las bases de datos de salud más grandes del mundo. Establecido en 1999 y puesto en práctica por el fondo nacional del seguro de salud para los empleados (CNAMTS), que contiene decenas de millones de datos sanitarios de solicitudes de reembolso de salud (hojas de cuidados clínicos, facturas, etc.). Las misiones se llevaron a cabo con CNAMTS y sus proveedores de servicios, así como con organizaciones que utilizan datos de SNIIRAM. Los hallazgos iniciales indican que la gestión del sistema generalmente es satisfactoria según la Ley de protección de datos. Sin embargo, la CNIL continúa su análisis sobre la seguridad y confidencialidad de los datos, dada la sensibilidad de este último y el número de personas involucradas.

Revendedores de datos: la CNIL ha llevado a cabo más de cincuenta auditorías sobre las diversas categorías de actores involucrados en la intermediación de datos, intermediarios que agregan, enriquecen, transforman y comercializan datos personales. Las auditorías identificaron a estos actores y su papel en el procesamiento de datos recopilados por algunos y reutilizados por otros. Las verificaciones se centraron en la base legal del tratamiento, las condiciones de recopilación de datos, los plazos de conservación, el conjunto de la

información de las personas y la facultad para que ejerzan sus derechos, así como las medidas de seguridad implementadas.

API-PNR: sistema API-PNR (Advanced Passenger Information - Passenger Name Record), el archivo de control de transporte aéreo permitido por la ley en modo de prueba en 2013, fue objeto de las primeras auditorías de los departamentos gubernamentales interesados. Sin embargo, dado el aplazamiento del despliegue final del sistema, los controles realizados por la CNIL continuarán una vez que se implemente el sistema, en 2017.

El 15% de las misiones se iniciaron a raíz de denuncias recibidas por la CNIL, por ejemplo, de empleados que informaron prácticas de vigilancia excesiva de su empleador (geolocalización, CCTV, etc.), pero también ciudadanos que se quejaron de recibir mensajes de prospección política o clientes que reportan dificultades para ejercer su derecho a oponerse a la recepción de mensajes publicitarios.

Más de la mitad de las auditorías fueron de seguimiento a temas alertados en la prensa, elementos recolectados durante auditorías previas, informes internos o externos.

La ley del 7 de octubre de 2016 para una República Digital ha multiplicado 20 veces el monto de las sanciones que puede emitir la CNIL (hasta 3 millones de euros). La regulación europea los multiplicará nuevamente, a partir de mayo de 2018, para alcanzar el 4% de la facturación global. También establece nuevos mecanismos de cooperación entre las autoridades europeas, comenzando con las operaciones conjuntas de auditoría.

Los temas que se abordaron en 2017, fueron:

La confidencialidad de los datos de salud procesados por las compañías de seguros: las compañías de seguros recopilan datos sobre el estado de salud de sus clientes, en el marco de muchos de sus contratos. Estos datos son un elemento esencial de la evaluación de riesgos que determina el compromiso de la aseguradora en el cumplimiento de la regulación. También se obtiene mucha información cuando un asegurado solicita una indemnización por un reclamo relacionado con su estado de salud. Un kit de cumplimiento fue publicado por la CNIL en

noviembre de 2014, que regula en particular el procesamiento de los datos de salud con respecto a la obligación de confidencialidad médica (secreto profesional). Hace referencia específica a la llamada convención "AERAS[104]", firmada por los diversos actores del sector para regular el uso de los datos de salud.

Este tema permitirá asegurar el cumplimiento por parte de las compañías de seguros de las reglas de confidencialidad de los datos de salud y con el respeto del secreto médico, dos años después de la implementación del kit de conformidad.

Archivos de inteligencia: varios archivos relacionados con la seguridad del Estado, la defensa o la seguridad pública estarán sujetos a auditorías por parte de la CNIL. Estos incluyen los archivos para la prevención de infracciones de seguridad pública autorizadas por decreto e implementadas por los servicios del Ministerio del Interior, en el que se transfirieron los antiguos archivos de información general: PASP (Prevención de Violaciones a la Seguridad Pública) Seguridad pública), GIPASP (Gestión de la información y prevención de ataques a la seguridad pública) y EASP (Investigaciones administrativas relacionadas con la seguridad pública).

Los controles cubrirán el funcionamiento general de estos archivos, así como el cumplimiento de las disposiciones reglamentarias aplicables. También se llevarán a cabo verificaciones en el archivo STARTRAC[105], que también está autorizado por decreto e incluye informes de sospechas de lavado de dinero transmitidas al servicio de competencia nacional de TRACFIN[106].

Smart TV's: Las televisiones y dispositivos conectados a Internet que ofrece nuevos servicios a los espectadores, como la actualización del sistema operativo de la propia TV,

[104] La Convención AERAS es un acuerdo firmado por miembros del gobierno, las aseguradoras y asociaciones de usuarios de los servicios de las aseguradoras, con el fin de constituir un organismo colegiado que permita controlar lo que estas empresas destinadas a brindar servicios de seguro, particularmente de salud, pueden llevar a cabo. Referencia completa en: http://www.aeras-infos.fr/files/live/sites/aeras/files/contributed/1.%20Convention_AERAS/Les_textes-de-reference/CONVENTIONAERAS2006.pdf Consultado el 12 de noviembre de 2016.

[105] Sistema automatizado de procesamiento de datos personales implementado por el servicio nacional de competencia TRACFIN.

[106] Es un servicio de inteligencia bajo la autoridad del Ministerio de Acción y Cuentas Públicas. Contribuye al desarrollo de una economía saludable luchando contra los circuitos financieros clandestinos, el lavado de dinero y el financiamiento del terrorismo.

video sobre demanda o el acceso a plataformas de video en línea. Permite al usuario interactuar a través de muchos medios incluso conectarse a sus redes sociales. Algunos modelos con tecnologías de reconocimiento de voz pueden analizar la voz del usuario para ejecutar sus instrucciones. Es probable que la información recopilada revele muchos aspectos de la privacidad de los usuarios, especialmente su estilo de vida y sus preferencias, como en el caso los algoritmos utilizados por Netflix[107].

Las auditorías efectuadas a estos proveedores y tecnologías abarcan el procesamiento de los datos recopilados por los televisores conectados, en particular la relevancia de la información recopilada, la revisión de la o las finalidades para el procesamiento llevado a cabo, así como las medidas de seguridad y confidencialidad implementadas.

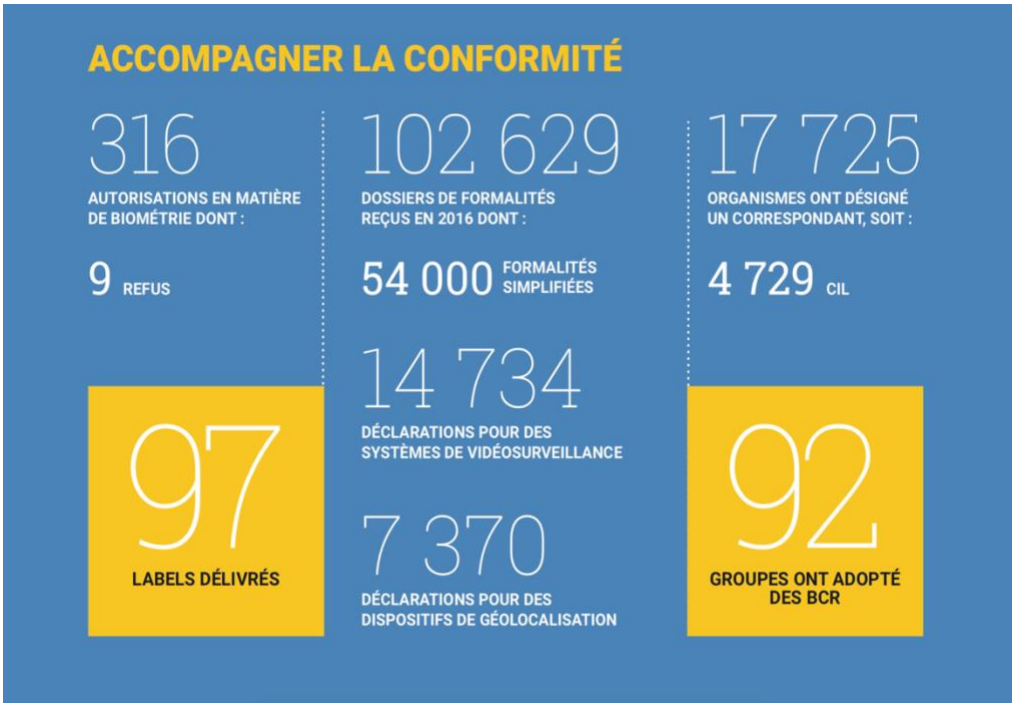
El año 2017 es un parteaguas no sólo para la CNIL, sino para todas las autoridades de protección de datos europeas por la entrada en vigor del GDPR.

Por último, algunas cifras reveladas por la propia CNIL en su reporte anual 2016[108], se presentan a continuación:

[107] En realidad, se trata de quince algoritmos diseñados para garantizarle al usuario el acceso a los contenidos que están más relacionados con sus preferencias, de tal suerte que siempre encuentre algo a su gusto y continúe utilizando la plataforma e incluso genere cierta dependencia. Más información disponible en: https://hipertextual.com/2016/04/tecnologia-de-netflix-algoritmos consultado el 12 de agosto de 2016.

[108] Reporte de actividades 2016 de la CNIL. En: https://www.cnil.fr/sites/default/files/atoms/files/cnil-37e_rapport_annuel_2016.pdf consultado el 7 de noviembre de 2017.


LES CHIFFRES CLÉS 2016
CONSEILLER & RÉGLEMENTER
3 078 DÉCISIONS ET DÉLIBÉRATIONS DONT :
190 AUTORISATIONS
145 AVIS
1 976 AUTORISATIONS DE TRANSFERT HORS UE (+83%)
697 AUTORISATIONS EN MATIÈRE DE SANTÉ (RECHERCHE ET ÉVALUATION)


ACCOMPAGNER LA CONFORMITÉ
316 AUTORISATIONS EN MATIÈRE DE BIOMÉTRIE DONT :
9 REFUS
97 LABELS DÉLIVRÉS
102 629 DOSSIERS DE FORMALITÉS REÇUS EN 2016 DONT :
54 000 FORMALITÉS SIMPLIFIÉES
14 734 DÉCLARATIONS POUR DES SYSTÈMES DE VIDÉOSURVEILLANCE
7 370 DÉCLARATIONS POUR DES DISPOSITIFS DE GÉOLOCALISATION
17 725 ORGANISMES ONT DÉSIGNÉ UN CORRESPONDANT, SOIT :
4 729 CIL
92 GROUPES ONT ADOPTÉ DES BCR

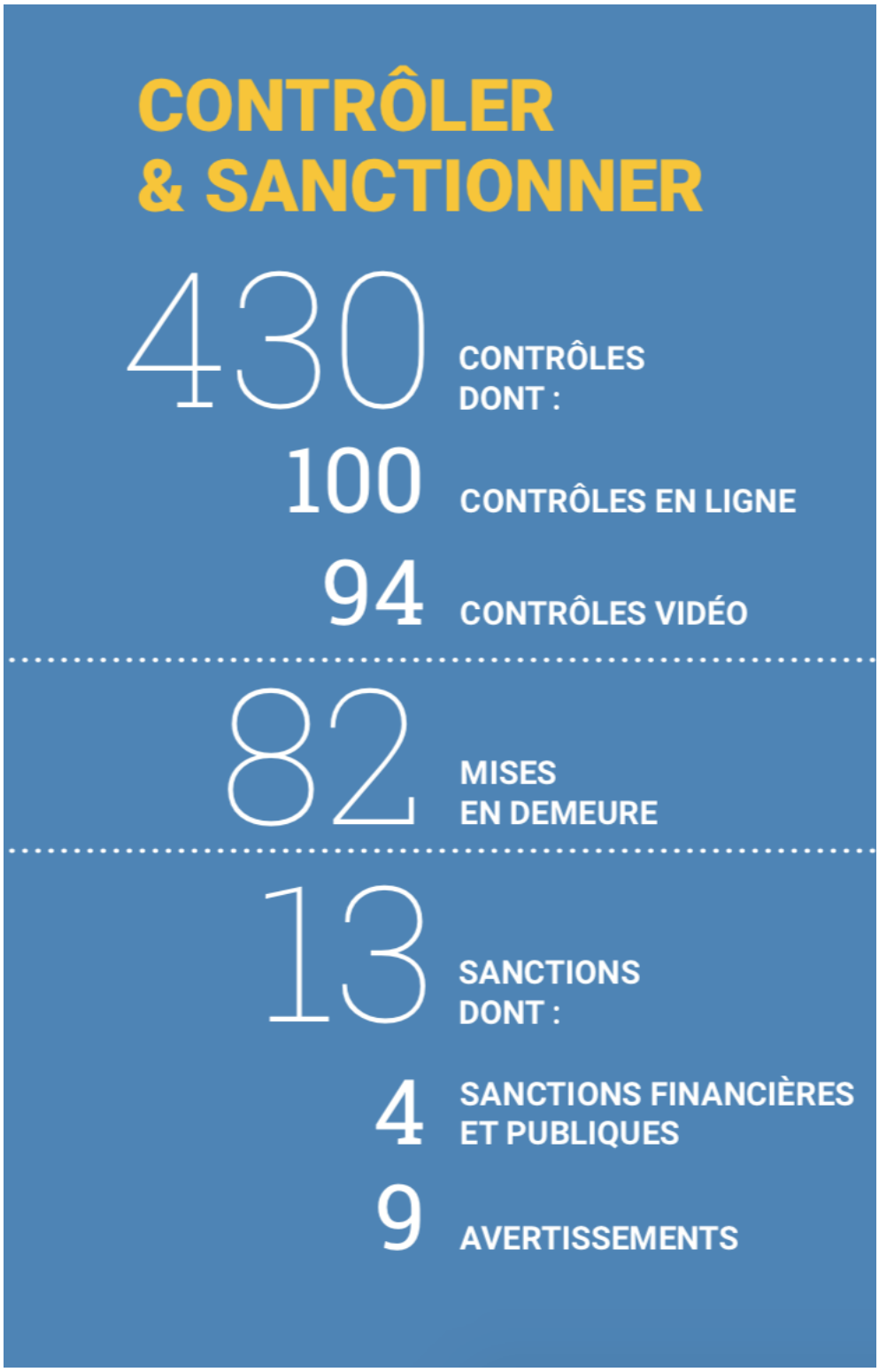


Fig. 9, 10 y 11 Cifras clave 2016, en relación a las acciones, decisiones y deliberaciones de la CNIL[109]

[109] Ibidem

CONCLUSIÓN DE LA PRIMERA PARTE.

A lo largo de esta primera etapa del presente trabajo doctoral presentamos las nociones básicas de la investigación, la parte toral de todo este esfuerzo: el concepto de identidad, así como los principios rectores de los sistemas jurídicos analizados.

Contrario a las ideas populares respecto de la lejanía de los criterios filosóficos y jurídicos de estos tres países, por razones de cultura, tradición legislativa o historia, podemos concluir que en materia de protección de datos personales, en realidad no somos tan distintos; es cierto, la legislación estadounidense sobrepone la seguridad nacional por encima de algunos derechos humanos, incluidos los que nos competen, a protección de los datos personales y la privacidad, en la medida de las posibles violaciones a la identidad del individuo; sin embargo, en la base, los tres países, a su modo, buscan a toda costa proteger a los titulares respecto del uso abusivo e injustificado se su información personal, lo que se constata en las cifras de las sanciones presentadas.

Esta primera sección abre la puerta de manera muy satisfactoria al resto de la investigación, ya que nuestro postulado inicial deriva de la hipótesis de que, al día de hoy, en el año de 2017, contamos con la regulación necesaria y pertinente que permite salvaguardar, al menos en los criterios indispensables, la identidad de los individuos.

SEGUNDA PARTE

IDENTIDAD DIGITAL. UN DESAFÍO A LA LEGISLACIÓN COMPLEMENTARIA.

CAPÍTULO I: IDENTIDAD DIGITAL Y DERECHO PENAL: CIBERCRIMEN.

Les lois les plus sages ont pour but naturel d'entendre à tous les hommes les avantages de l'existence et de combattre tout ce qui tend à les concentrer sur un petit nombre et à accumuler d'un côté la puissance et le bonheur, et de l'autre la faiblesse et la misère.
Cesare Beccaria, 1764.

Es bien sabido, que el derecho siempre va un paso atrás de la innovación y los cambios sociales, el derecho penal históricamente va un paso más atrás, ya que primero hace falta reconocer la importancia del derecho que hay que defender, para reconocerle una tutela jurídica por parte del Estado y sancionar a aquél que ose vulnerarlo.

La sociedad de la información llegó a nuestras vidas y las de nuestros padres de manera vertiginosa e intempestiva, antes de darnos cuenta ya estábamos inmersos en ella, algunas veces maravillándonos de la magia que supone para el ser humano moderno, hacer cosas que a principios del siglo pasado serían únicamente ciencia ficción y otras más, simplemente dejándonos llevar por la ola social y emocional tan exitante que nos ofrece esta sociedad moderna.

Internet brinda acceso a la información y la palabra a los ciudadanos más que ningún otro medio existente. La volatilidad de los sitios y el relativo anonimato que permite, se transforma en un auténtico vehículo que da la impresión de libertad. Sin embargo, a la inversa, Internet ¿será acaso la encarnación tecnológica de la famosa bestia del apocalipsis?[110].

[110] Beson, Éric "La République numérique", Grasset, 2008

No podemos satanizar a la tecnología, pero es muy cierto que Internet abrió las puertas a mundos y conductas con las que no estábamos tan familiarizados y hemos tenido que aprender en el camino a prueba y error, usuarios, gobierno, profesionales de la tecnología y juristas.

La experiencia muestra que una gran parte de los juristas, incluyendo abogados litigantes, legisladores y jueces, en prácticamente todo el mundo frente a las tecnologías de la información se muestran en ocasiones perplejos ante el funcionamiento vertiginoso, volátil y casi místico de las redes y en general del entorno informático.

La diferencia cultural y conceptual entre la ciencia detrás de los avances tecnológicos y los principios generales del derecho, se ha convertido en uno de los principales frenos contra el fenómeno de la cibercriminalidad, es por ello que los abogados tenemos que abrir nuestra mente a las opciones y nuevos paradigmas que ofrece la evolución tecnológica para poder disfrutar de las nuevas maneras de hacer el bien y de atacar el mal.

El derecho penal aplicado a las tecnologías de la información y la comunicación, ha comenzado a constituir un binomio cada vez más frecuente, por desgracia, debido al incremento de las actividades ilícitas cometidas a través de estos nuevos medios.

La irrupción de un mundo digital a nuestra vida o viceversa, ha versado en una serie de componentes normativos incluso de carácter penal. Esa frontera entre el bien y el mal, que en este mundo virtual llega a ser tan tenue y que es trabajo del derecho penal delimitar pasa a veces desapercibida en el terreno de Internet.

Más allá de una simple adaptación de una arquitectura penal clásica, donde los roles y los límites de las conductas estaban perfectamente delimitados, ahora, todas las partes implicadas deberán adaptarse a un cambio de hábitos.

Lo innegable es que el derecho penal se encuentra cara a un nuevo entorno, semidesconocido que no puede pasar por alto, este entorno es lo que se conoce como el

"ciberespacio".

El delito está íntimamente ligado a la manera de ser de cada pueblo y a las necesidades de cada época, los hechos que han tenido alguna vez ese carácter, lo han perdido en función de situaciones diversas y al contrario, acciones no delictuosas, han sido erigidas en delitos[111].

1.1 LA CIBERCRIMINALIDAD

El concepto cibercriminalidad, no ha quedado suficientemente claro para casi ninguna autoridad a nivel internacional; el prefijo "ciber", proviene de una palabra griega kubernan, que en griego significa gobernar, y que también se encuentra presente en la palabra cibernética[112]

Este prefijo "ciber" acompaña muchas de las palabras contemporáneas que los internautas estamos utilizando en el día a día, como ciberamigo, cibercafé, cibernovio, ciberataques, etc.

Asimismo, este prefijo es la base de la palabra que nos compete que es cibercriminalidad, que se asocia a la delincuencia llevada a cabo a través de medios informáticos. Hoy en día se utiliza para denominar diversas actividades delincuenciales como ciberfraude, ciberbullying o ciberterrorismo.

El cibercrimen continúa siendo una noción abstracta para los juristas, toda vez que ni la Convención sobre la Ciberdelincuencia del Consejo de Europa [113] define

---

[111] Castellanos, Fernando "Lineamientos elementales de Derecho Penal", Porrúa 1990, México. P. 125.

[112] Sobre la cibernética, hay al menos una cosa en la que todos están de acuerdo: esta palabra deriva de una palabra griega, *kubernêtik*ê, que Platón solía referirse al pilotaje de un barco. A menudo ha usado esta metáfora para presentar el verdadero arte de gobernar, el basado en la sabiduría, en el conocimiento del bien.

"La cibernética es el arte de hacer efectiva la acción". Esta definición de Couffignal, un pionero francés de la cibernética, es la más cercana a la concepción de Platón. El buen piloto es aquel cuya acción es efectiva en la tormenta. "Ciencia del control y la comunicación en los animales y la máquina. Esta es la definición de Norbert Wiener, el autor Cibernética o control y comunicación en el animal y la máquina, un libro publicado en 1948. A este estadounidense le atribuimos la paternidad de la cibernética. En: http://agora.qc.ca/dossiers/Cybernetique. Consultado el 20 de marzo de 2015.

[113] Convenio sobre la Ciberdelincuencia del Consejo de Europa, o Convención de Budapest del 23 de noviembre de 2001. En: https://rm.coe.int/16802fa41c. Consultado el 21 de marzo de 2015.

claramente, a pesar de que sí define diversas conductas ilícitas que encuadran en ese concepto.

El término cibercrimen definido por la Interpol es el siguiente:

"*El cibercrimen es un tipo de crímenes de rápido crecimiento. Cada vez son más los criminales que están explotando la velocidad, comodidad y anonimato de Internet para cometer una diversidad de actividades criminales que no conocen fronteras, este tipo de crimen ya sea físico o virtual, provoca daños graves y plantean amenazas muy reales a las víctimas en todo el mundo.*

Aunque no existe una definición universal única de delito cibernético, la aplicación de la ley generalmente hace distinción entre dos tipos de delitos relacionados con Internet:

Cibercrimen avanzado (o crimen de alta tecnología): ataques sofisticados contra el hardware y software de la computadora;

Delitos informáticos: crímenes "tradicionales" que han tomado un nuevo rumbo con el advenimiento de Internet, como los crímenes contra los niños, los delitos financieros y hasta el terrorismo.

Las organizaciones criminales recurren a Internet para facilitar sus actividades y maximizar sus ganancias en el menor tiempo. Los crímenes en sí mismos no son necesariamente nuevos, como el robo, el fraude, el juego ilegal, pero se están generalizando y son más dañinos."

Desde la perspectiva francesa, un ciberataque se define por el gobierno francés como:

"Un ataque cibernético es un intento de atacar sistemas informáticos hechos para propósitos maliciosos. Puede tener como objetivo robar datos, destruir, dañar el funcionamiento normal de los dispositivos informáticos, tomar el control de los procesos

informáticos o dispositivos de autenticación engañosos para realizar operaciones ilegítimas[114]*."*

Miguel Ángel Davara define al Delito Informático como *"…la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"*.

En la legislación mexicana estas conductas ilícitas se han planteado a nivel doctrinal como delitos informáticos, el Código Penal del Estado de Sinaloa, fue el primero en incluir en su catálogo, el término delito informático, si bien, la redacción es muy poco afortunada, se considera un antecedente importante en materia de innovación legislativa, para su momento.

> *"Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:*
>
> *I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o*
>
> *II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.*
>
> *Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa."*

Existen diversos tipos de conductas delictivas contempladas en nuestra

[114] Cyberattaque. En: http://www.gouvernement.fr/risques/lexique/lettre_c#parentVerticalTab16. Consultado el 25 de noviembre de 2017.

legislación mexicana.[115]

1.2. LOS DIFERENTES ROSTROS DE LA USURPACIÓN DE IDENTIDAD.

A pesar de que la práctica de la conducta ilícita que hoy conocemos como usurpación o robo de identidad, es bastante añeja; los ojos de México y del mundo, han volteado hacia esta problemática por dos principales razones: las grandes pérdidas económicas y su creciente multiplicación en casos.

Como precisamos en el párrafo anterior, esta conducta ilícita, en términos de lo que universalmente se reconoce como tal, es decir, algo contrario a la moral, falto de ética o prohibido por la Ley; no es un comportamiento novedoso, sin embargo, ha cobrado un mayor auge gracias a las nuevas tecnologías, ya que por una parte su comisión se ha vuelto más rápida y sencilla, y por la otra, también es cierto que gracias a la tecnología, es más fácil y rápido descubrir un ataque de esta naturaleza y difundir la noticia del mismo.

Como lo hemos explicado anteriormente, lo que conocemos como identidad está compuesta de muy diversos factores, tanto jurídicos como fisiológicos, genéticos, históricos, psicológicos e incluso hasta espirituales o religiosos, pero todos estos elementos nos individualizan y nos identifican diferenciándonos de otros en la sociedad en la que nos desenvolvemos. El tema de la usurpación de identidad es cada vez más relevante, en primera por la tendencia a su incremento en todas partes del mundo, y en segunda y quizás la más importante, por todos los bienes jurídicos tutelados que se vulneran con este acto ilícito.

La identidad, sin duda alguna, está compuesta de diversos elementos, características, credenciales, documentos, información, datos personales, hábitos, contraseñas, que nos dan acceso a un sinnúmero de derechos, privilegios, actividades, lugares, etc. Nuestra identidad de alguna manera marca y define nuestro lugar en el mundo; es por ello que cada vez se vuelve más atractiva para los malhechores o delincuentes, dado que es una puerta de entrada a nuestro mundo, esa puerta puede ser tan grande o limitada como el atacante tenga oportunidad, es decir, que mientras más información posea de nosotros y más control sobre ella pueda ejercer, mayor será el potencial daño hacia nuestra

[115] Ver anexo III.

persona.

Jurídicamente, la identidad se encuentra regulada y protegida por tratados internacionales en materia de Derechos humanos y desde luego la legislación de los tres países parte de este estudio, en la declaración de los Derechos de Hombre y el Ciudadano de 1789, se reconocen mediante declaración solemne, los derechos naturales, inalienables y sagrados del Hombre[116], tal es el caso el derecho la identidad personal.

La Declaración de los derechos del hombre

Desde el año 1488, Estados Unidos

Lo que en adelante describiremos indistintamente como usurpación, suplantación o robo de identidad, es en sí una actividad ilícita que nunca viene sola, es decir, siempre existe un momento antes y después de la comisión de este delito; el primer momento es el de la obtención de la información, el cual puede darse de forma lícita o ilícita, por ejemplo: no es lo mismo el caso de aquél que obtiene identificadores de una persona al momento de asaltarla en la calle y robarle su cartera, que otro caso en el cual un empleado de una empresa de servicios de telefonía, obtiene lícitamente una serie de identificadores necesarios para la generación de un contrato de prestación de servicios, y que posteriormente, realiza un tratamiento ilícito de esa información para fines distintos a los originarios suplantando la identidad del titular de los datos personales para entonces, cometer otro ilícito, el cuál puede ser de múltiples naturalezas.

En todo caso, no es una conducta ilícita aislada, pues desde el momento en que un sujeto planea la suplantación de identidad de otro, en la mayoría de los casos lo hace como un medio para la comisión de otro delito, el cual no sería posible de llevar a cabo si no fuera porque la identidad de la víctima ha sido suplantada.

A nivel internacional, particularmente en los países que forman parte del presente estudio, la conducta ilícita que describimos, puede ser denominada de distintas maneras, las cuales enlisto a

[116] « *Déclaration solennelle, les droits naturels, inaliénables et sacrés de l'Homme* » (http://www.assemblee-nationale.fr/connaissance/constitution.asp#declaration).

continuación:

1. Usurpación de identidad;
2. Robo de identidad;
3. Suplantación de identidad.

Procederemos a analizar cada una de las nomenclaturas dadas, para determinar cuál consideramos más idónea para describir exactamente la conducta; esto aunque pudiera ser irrelevante o un simple aspecto formal, tiene un profundo sentido ya que si el concepto no obedece de forma pertinente a la naturaleza de la conducta, es muy probable que no sólo el juzgador, sino el legislador de las nuevas generaciones no pueda incorporar este tipo penal en las diversas legislaciones a que haya lugar, o en su caso imponer sanciones administrativas para conductas tendientes a la comisión de este ilícito.

En primer lugar, tenemos al concepto de usurpación de identidad, el cual se encuentra presente en distintos tipos penales contenidos en códigos penales mexicanos y en el código penal francés. Ahora bien, procederemos a desmembrar este concepto.

El término usurpación, proviene del latín *usurpatio*, que a su vez tiene sus orígenes en el Derecho Romano, y está íntimamente vinculada al patrimonio, a la posesión de bienes generalmente inmuebles, en este preciso momento nos encontramos ante la primera disyuntiva, ya que, como lo planteamos anteriormente, la identidad como un todo complejo, no es susceptible de ser un bien mueble o inmueble, es decir, es más un derecho humano y personalísimo que un derecho real, por lo tanto, darle el carácter de "cosa", desde mi particular punto de vista, sería casi como minimizar el daño causado a la víctima, ya que no es un efecto cuantificable únicamente en dinero, sino en repercusiones psicológicas y en muchos casos también físicas, y no sólo patrimoniales.

Otro punto importante es que aquello a lo que llamamos comúnmente como "usurpación de identidad", en la mayoría de los casos se trata de "usurpación de identificadores o de credenciales en lo particular" y no de la identidad en sí misma; por ejemplo, cuando una persona utiliza una tarjeta de crédito de otra sin su consentimiento o la clona, para realizar compras a nombre de la víctima pero sin su conocimiento y desde luego sin su consentimiento, estamos ante la presencia de la utilización ilícita de un medio de pago y en su caso de un fraude a terceros valiéndose de un instrumento cuya posesión debería siempre estar en manos de su titular legítimo; sin embargo, eso no significa

que el atacante haya cobrado por completo la posesión de la personalidad de la víctima, sino únicamente de uno de sus medios de pago o credenciales bancarias para un fin específico, que no impidió que la víctima continuara gozando de todos los elementos de su identidad, tan es así, que en la mayoría de los casos como el que describimos, la víctima no se entera de lo ocurrido hasta mucho después, incluso podría haber estado usando esa misma tarjeta para comprar en otro establecimiento al mismo tiempo que el atacante.

El poder que se tiene sobre los identificadores ya sea en el mundo real o virtual, depende del tipo de ataque, por ejemplo, cuando una persona es víctima de un ataque de phishing, y con motivo de este engaño comparte su contraseña de una red social, por ejemplo, Facebook, o bien, estos terceros pueden tomar el control de la cuenta y publicar en su nombre, pero este control únicamente se refiere a uno de sus identificadores virtuales, no a su identidad per se; Pedro López, no deja de ser Pedro López ni pierde todos los atributos de su personalidad e identidad por haber perdido o cedido el control de su identidad virtual en Facebook, y en la mayoría de los casos cuando la víctima descubre estos hechos en poco tiempo y bajo las mismas políticas de carácter privado implementadas por la propia plataforma, ésta puede recuperar en un tiempo razonable el control sobre su cuenta.

Hacemos esta reflexión, porque una vez más, buscamos que la nomenclatura asignada a este ilícito que nos ocupa, sea la más precisa e idónea atendiendo a la naturaleza de la conducta y de sus elementos.

La usurpación es definida por la Real Academia Española como:

> "1. f. Acción y efecto de usurpar.
> 2. f. Cosa usurpada, especialmente el terreno usurpado.
> **3. f. Der. Delito que se comete apoderándose con violencia o intimidación de inmueble o derecho real ajeno."**

Por lo tanto, la última de sus acepciones nos remite indefectiblemente al terreno de los derechos reales, es decir, aquellos que versan sobre una cosa en este caso inmueble, por lo que, si comprendemos a los identificadores o credenciales como una cosa, en particular, por su naturaleza un bien equiparable al mueble en términos del artículo 759 del Código Civil Federal, el término usurpación sería ciertamente incorrecto.

Sin embargo, en México, el término usurpación de identidad es reconocido como correcto, tan es así que se encuentra tipificado en los siguientes ordenamientos penales estatales de nuestro país:

1. Código Penal para el Distrito Federal.

En el Diario de los Debates de la Asamblea Legislativa del Distrito Federal, del día 29 de junio de 2010, en la sesión extraordinaria presidida por el Diputado Julio César Moreno Rivera, se expuso el Dictamen relativo a la iniciativa de reforma, con proyecto de decreto, por la que se crea un capítulo III en el título décimo segundo del Código Penal para el Distrito Federal, con la finalidad de tipificar el delito de **usurpación de identidad o personalidad**. El cual, en abril del mismo año había sido presentado por el Diputado del Partido Revolucionario Institucional Diputado Octavio West Silva, la cual posteriormente sería analizada por la Comisión de Administración Y Procuración de Justicia en el ejercicio de sus facultades constitucionales.

Respecto de las razones de la reforma planteada, el Diputado West Silva, en su exposición de motivos planteaba lo siguiente:

> *"En la actualidad, el fácil acceso a los medios electrónicos, los avances tecnológicos, las llamadas redes sociales y el uso de servicios de banca por Internet, se han constituido en una herramienta primordial para aquellos que adoptan la identidad de un tercero, normalmente para cometer algún ilícito, para ocultarse o para evadirse de la acción de la justicia. La utilización de datos a través de redes sociales, correos electrónicos, solicitudes de servicios, trámites públicos y privados, etcétera; mediante los cuales se aporta información personal a terceros aparentemente "confiables", para los usuarios, permite que los delincuentes obtengan de manera sencilla los datos para realizar esta nueva modalidad de afectación contra la Seguridad de las Personas, constituyéndose en una actividad a todas luces ilícita."*
>
> *En la actualidad no existen propuestas que tipifiquen este tipo de conductas para sancionar su comisión; independientemente de que conducta de Usurpación de Personalidad o Identidad, sea el medio para la comisión de otros delitos o la forma de ocultarse o evadirse por haber incurrido en otras conductas delictivas, debe ser tipi cada y penada como un delito autónomo, aun cuando pudiera existir un concurso de delitos como podrían ser la alteración de documentos públicos o privados, falsificación, fraude, lavado de dinero, evasión de presos, fraude procesal,*

crimen organizado, entre otros."

A juicio de la Comisión Dictaminadora de la Asamblea Legislativa, efectivamente no existía regulación de la citada conducta ilícita en el Código Penal; por lo tanto, acordó procedente la creación de un tipo penal que sancionara la usurpación de personalidad o identidad (sic).

En un primer momento, la iniciativa planteada consistía en la adhesión de los artículos 211 Bis, 211 Ter Y 211 Quáter; en el siguiente sentido:

> ***Artículo 211 Bis.*** *- Al que por cualquier medio usurpe la personalidad o identidad de otra persona, independientemente de la nalidad que persiga con la comisión de esta conducta, se le impondrá una pena de dos a seis años de prisión y de cuatrocientos a seiscientos días multa.*
>
> *Al que otorgare su consentimiento para ser suplantado por un tercero en su persona o identidad, se le considerará igualmente responsable del delito previsto en el párrafo anterior, aplicándose las mismas penas que al usurpador.*
>
> ***Artículo 211 Ter.*** *- Comete el delito de Usurpación de Personalidad o identidad, el que con el objeto de suplantar a otro, se acredite con la personalidad de éste, alterando, reproduciendo, falsificando, utilizando o proporcionando, ante terceros, la siguiente información o documentos personales del suplantado:*
>
> ***I.-*** *Nombre;*
>
> ***II.-*** *Número de Seguridad Social;*
>
> ***III.-*** *Registro Federal de Contribuyentes;*
>
> ***IV.-*** *Clave Única de Registro de Población;*
>
> ***V.-*** *Clave de Elector;*
>
> ***VI.-*** *Números de Tarjeta de Crédito, números confidenciales y/o claves de acceso a servicios de banca por Internet, telefónicos o cualquier otro dato o elemento que permita el acceso a los servicios bancarios del afectado.*
>
> ***VII.-*** *Tarjetas de Crédito o plásticos bancarios del titular o adicionales;*
>
> ***VIII.-*** *Chequeras del titular de cuenta;*
>
> ***IX.-*** *Actas de Nacimiento o del Estado Civil;*
>
> ***X.-*** *Credencial para votar con fotografía o de elector;*

XI.- *Licencia de conducir;*

XII.- *Pasaporte;*

XIII.- *Cédulas Profesionales*

XIV.- *Títulos Profesionales, Certificados o Constancias de Estudios;*

XV.- *Credenciales Escolares o laborales;*

XVI.- *Declaraciones Fiscales;*

XVII.-*Documentos o Constancias laborales;*

XVIII.- *Expedientes públicos o judiciales;*

XIX.-*Boletas Prediales; Recibos de Agua, Teléfono, Suministro de Energía Eléctrica; Estado de Cuenta Bancarios y/o de Servicios;*

XX.- *Poderes Notariales;*

XXI.- *Huellas dactilares;*

XXII.- *Grabaciones de voz;*

XXIII.- *Imágenes de retina;*

XXIV.- *Número de teléfono celular, de o cina, domicilio o cualquier otro que permita la ubicación del titular;*

XXV.- *Firma Autógrafa;*

XXVI.- *Firma Electrónica;*

XXVII.- *Cualquier otra información o documento que identifique física o electrónicamente a un individuo; o permita el acceso a sus bienes o patrimonio o responsabilidades.*

Artículo 211 Quáter .- *En caso de que quien usurpe la personalidad o identidad de otro, se valga para ello de una homonimia, de la igualdad física genética entre hermanos gemelos, o del parecido físico con el suplantado, para cometer el ilícito, se aumentarán en una mitad las sanciones previstas en el Artículo 211 Bis, para este delito.*

De la redacción original del proyecto de reforma, en particular a lo que se refiere al artículo 211 Ter, logramos inferir que el legislador atinadamente pretendía regular el uso no autorizado de identificadores, documentos o credenciales más que de lo que se conoce como identidad o personalidad en su conjunto y correcta dimensión.

Con base a la reforma se crea el Capítulo III del Título Décimo Segundo del Código Penal del Distrito Federal de los Delitos contra la paz, la seguridad de las personas y la inviolabilidad del domicilio, el tipo penal de usurpación de identidad quedó como sigue:

> ***Articulo 211 Bis***. *- Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.*
>
> *Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo.*

En términos de la redacción vigente del artículo, la conducta ilícita consiste en usurpar la identidad de otro, con la condicionante de que ésta se haga con fines ilícitos, luego entonces, para romper el elemento de antijuridicidad, debería existir un fin lícito, a no ser que se tratara de salvaguardar la vida o la integridad humana, no parece sencillo ni aparente algún caso de esta naturaleza, asimismo, el sujeto activo también podría ser aquél que autoriza a otro a ser suplantado en su identidad. Aunado a esto se presenta como agravante de la conducta quien se valga de la homonimia, parecido físico o similitud de la voz para la comisión del delito, es decir, de elementos que lo pongan en situación de ventaja frente a la víctima u ofendido.

2. Código Penal el Estado de México

El Código Penal del Estado de México, también reconoce a la usurpación de identidad como una conducta ilícita, describiéndola de la siguiente manera:

> ***Artículo 264***.- *Se le impondrán de uno a cuatro años de prisión y de cien a quinientos días multa, a quien ejerza con fines ilícitos un derecho o use cualquier tipo de datos, informaciones o documentos que legítimamente pertenezcan a otro, que lo individualiza ante la sociedad y que le permite a una persona física o jurídica colectiva ser identificada o identificable, para hacerse pasar por él.*

Se equiparan a la usurpación de identidad y se impondrán las mismas penas previstas en el párrafo que precede prevista en el presente artículo a quienes:

I. Cometan un hecho ilícito previsto en las disposiciones legales con motivo de la usurpación de la identidad;

II. Utilicen datos personales, sin consentimiento de quien deba otorgarlo;

III. Otorguen el consentimiento para llevar a cabo la usurpación de su identidad; y

IV. Se valgan de la homonimia para cometer algún ilícito.

Las sanciones previstas en este artículo se impondrán con independencia de las que correspondan por la comisión de otro u otros delitos.

***Articulo 265**.- Las penas señaladas en el artículo anterior se incrementarán hasta en una mitad, cuando el ilícito sea cometido por un servidor público aprovechándose de sus funciones, o por quien sin serlo, se valga de su profesión o empleo para ello.*

No es de sorprendernos la forma en la que el legislador colimense aborda esta problemática de forma objetiva y desde otra perspectiva quizás más práctica respecto de lo que en términos generales hemos denominado usurpación de identidad, en este caso, el Código Penal para el Estado de Colima, equipara esta conducta al fraude de la forma que a continuación se describe:

***Artículo 201**. Se considera fraude y se impondrá pena de cuatro a once años de prisión y multa por un importe al equivalente de cuatrocientos cincuenta a mil días de salario mínimo, en los siguientes casos:*

*… **III**. **Uso Indebido de tarjetas y documentos de pago electrónico**. Al que sin el consentimiento de su titular o de quien esté facultado para ello, haga uso de una tarjeta, título, documento o instrumento de pago*

electrónico, bien sea para disposición en efectivo o para el pago de bienes y servicios.

Igual pena se impondrá a quien teniendo el consentimiento de su titular o de quien esté facultado para ello, haga un uso indebido de tarjetas, títulos, documentos o instrumentos de pago electrónico, bien sea para el pago de bienes y servicios o para disposición en efectivo.

***VI. Uso indebido de información confidencial o reservada de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición en efectivo**. A quien obtenga un lucro en perjuicio del titular de una tarjeta, título, documento o instrumento para el pago electrónico de bienes y servicios o para la disposición de efectivo, mediante la utilización de información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir los mismos.*

Si el sujeto activo es empleado o dependiente del ofendido, la pena de prisión se aumentará de dos a cinco años.

***VII. Manipulación indebida informática**. Al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido para sí o para otro valiéndose de alguna manipulación informática, instrucciones de código, predicción, intercepción de datos de envío, reinyecte datos, use la red de redes montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados, imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecte la confiabilidad, y variación de la navegación en la red o use artificio semejante para obtener lucro indebido.*

De igual forma, la misma sanción del párrafo anterior se impondrá, a quien intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

En el supuesto que el activo tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines, la pena se aumentará hasta en cuatro años más, además de una inhabilitación o suspensión para ejercer su profesión por un término igual al de la pena de prisión impuesta.

En definitiva, el legislador colimense, alcanza a percibir que el fin último del delincuente que suplanta la identidad de otro aprovechándose de la información personal de éste, así como sus identificadores, es el de cometer un acto fraudulento, que le signifique algún tipo de ganancia o lucro indebido. Esto confirma, que el fin último del sujeto activo no es en sí llevar a cabo la conducta de suplantación de identidad, sino aquello que puede obtener mediante ésta, cometiendo así, una multiplicidad de conductas ilícitas.

INICIATIVAS DE REFORMA AL CÓDIGO PENAL FEDERAL RELACIONADAS CON EL DELITO DE USURPACIÓN DE IDENTIDAD.

El incremento voraz en la incidencia de esta conducta delictiva en nuestro país, ha despertado el interés del legislador, por incorporar este tipo penal en el catálogo de delitos federales, sin embargo, hasta la fecha, es decir, finales de 2017, no ha tenido éxito, a continuación, presentamos una tabla con las propuestas efectuadas.

Año	Propuesta	Cámara de Origen	Estatus
2014	Capítulo III Robo de identidad Artículo 287 Bis. Al que por cualquier medio suplante con fines ilícitos o de apropiamiento de datos personales, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la suplantación en su identidad, se le impondrá una pena de uno a cinco años de prisión, de cuatrocientos a seiscientos días multa y, en su caso, la reparación del daño que se hubiere causado, en los términos del artículo 29 de este	Diputados	Inconclusa

	Código. Serán equiparables al delito de robo de identidad y se impondrán las mismas penas previstas en el párrafo que precede, las siguientes conductas: I. Al que por algún uso de los medios informáticos o electrónicos, valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a bases de datos automatizadas para suplantar identidades, con el propósito de generar un daño patrimonial u obtener un lucro indebido para sí o para otro; II. A quien transfiera, posea o utilice, sin autorización, datos identificativos de otra persona con la intención de cometer, intentar o favorecer cualquier actividad ilícita; III. Al que asuma, suplante, se apropie o utilice a través de internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca; y IV. Al que porte o utilice para identificarse ante cualquier persona física o moral, un documento expedido por autoridad nacional o extranjera, que haya sido alterado para suplantar la identidad de su titular.		

	Las penas previstas en el presente artículo se impondrán sin perjuicio de las que correspondan por los delitos que resulten, aplicándose al efecto las reglas del concurso real.		
2016	"Artículo 430. Comete el delito de usurpación de identidad al que por sí o por interpósita persona, usando cualquier medio lícito o ilícito, se apodere, apropie, transfiera, utilice o disponga de datos personales sin autorización de su titular o bien suplante la identidad de una persona, con la finalidad de cometer un ilícito o favorecer su comisión. "Se impondrá una pena de uno a seis años de prisión y de cuatrocientos a seiscientos días multa y, en su caso, la reparación del daño que se hubiera causado, a quien cometa el delito de usurpación de identidad. "Las penas previstas en el párrafo anterior se aumentarán hasta en una mitad cuando el ilícito sea cometido por un servidor público que aprovechándose de sus funciones tenga acceso a bases de datos o por quien se valga de su profesión para ello".	Diputados	Inconclusa
2017	INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA EL ARTÍCULO 430 AL CÓDIGO PENAL FEDERAL.	Senadores	Inconclusa

	Título Vigésimo Séptimo Delito contra la Identidad de las Personas Usurpación de Identidad Artículo 430. Se impondrá pena de uno a seis años de prisión y de cuatrocientos a seiscientos días multa al que por algún medio informático usurpe, asuma, transfiera, utilice, se apodere, suplante o se apropie de la identidad de otra persona sin autorización para el uso ilícito de sus datos personales generando un daño en su patrimonio con el fin de obtener un lucro para sí o para otro. Se aumentarán las penas previstas en el presente artículo hasta en una mitad cuando el delito sea cometido por algún servidor público que aprovechándose de sus funciones use ilícitamente datos personales a los que tenga acceso, asimismo, si el sujeto activo cuenta con un grado académico dentro del rubro de la telemática o informática se aplicará la privación del ejercicio de su actividad profesional. Si al usurpar la identidad se hiciere uso de la información se acumularán la pena de usurpación de identidad y el delito que por medio de ella hubiere cometido el delincuente.		
2017	Artículo 211 Quintus. Usurpación de Identidad Ajena. A quien usurpe, suplante, obtenga, utilice, apropie o adopte la identidad de otra persona, a	Diputados	Presentada

	través de un sistema informático con la intención de causar un daño o perjuicio a una persona, se le impondrá pena de uno a cinco años de prisión y de cuatrocientas a seiscientas veces el valor diario de la Unidad de Medida y Actualización. La misma pena se impondrá cuando la usurpación de identidad ajena se cometa infringiendo medidas de seguridad y con la intención de obtener de forma ilegítima un beneficio económico o lucro indebido para sí mismo o para otra persona o generar un daño en el patrimonio de una persona tanto física como jurídica.		

Para el derecho anglosajón, el robo de identidad o el fraude sobre la identidad, es justamente eso, un tipo novedoso o diferente de fraude, pero fraude, al fin y al cabo.

¿Qué son el robo de identidad y el fraude de identidad?

El robo de identidad y el fraude de identidad son términos utilizados para referirse a todos los tipos de delitos en los que alguien obtiene y usa los datos personales de otra persona de una manera que involucra fraude o engaño, generalmente con fines de lucro.

Muchas personas responden al "spam" o correo electrónico no solicitado, que les promete algún beneficio, pero solicita datos de identificación, sin darse cuenta de que, en muchos casos, el solicitante no tiene la intención de cumplir su promesa. En algunos casos, los delincuentes han utilizado tecnología informática para robar grandes cantidades de datos personales.

Con suficiente información de identificación sobre una persona, un delincuente puede hacerse cargo de la identidad de esa persona para llevar a cabo una amplia gama de delitos. Por ejemplo:

- Solicitudes de préstamos y tarjetas de crédito,
- Retiros fraudulentos de cuentas bancarias,
- Obtener cualquier clase de privilegios a los que no tiene derecho.

Existen varios tipos comunes de robo de identidad detectados en Estados Unidos:

Robo de identidad de menores: las identificaciones de los niños son vulnerables porque el robo puede pasar desapercibido durante muchos años. Para cuando son adultos, el daño a su identidad ya está hecho.

Robo de identificación de impuestos: un ladrón utiliza su número de seguridad social para presentar falsamente declaraciones de impuestos ante el Servicio de Impuestos Internos o ante el gobierno estatal.

Robo de identidad médica: esta forma de robo de identidad ocurre cuando alguien roba su información personal, como su número de identificación de Medicare[117] o su número de seguro médico para obtener estos servicios o para emitir una factura fraudulenta a su proveedor de seguro médico.

Robo de identidad a personas mayores: robo de identidad que se dirige a personas mayores o ancianos. Las personas de edad avanzada son vulnerables al robo de identidad porque están en contacto más frecuente con los profesionales médicos que obtienen su información de seguro médico, o los cuidadores y el personal en centros de atención a largo plazo que tienen acceso a información personal o documentos financieros, o bien, no se encuentran correctamente familiarizados con el uso seguro de las nuevas tecnologías.

Robo de identidad social: un ladrón usa su nombre, fotos y otra información personal para

[117] Medicare es el programa federal de seguro médico de los Estados Unidos de América, para personas de al menos 65 años de edad, personas más jóvenes con incapacidades y personas con enfermedad renal terminal (insuficiencia renal crónica que requiere diálisis o trasplante, a veces denominada ESRD).

crear una cuenta falsa en una plataforma de redes sociales.

El Departamento de Justicia de los Estados Unidos procesa los casos de robo de identidad y fraude bajo una variedad de estatutos federales. En el otoño de 1998, por ejemplo, el Congreso aprobó la Ley de robo de identidad y disuasión de suposiciones (Identity Theft and Assumption Deterrence Act) ITADA[118]. Esta legislación creó un nuevo delito de robo de identidad, que prohíbe "transferir intencionalmente o usar, sin autorización, un medio de identificación de otra persona con la intención de cometer, o ayudar o instigar, cualquier actividad ilegal. eso constituye una violación de la ley federal, o constituye un delito grave bajo cualquier ley estatal o local aplicable ". 18 U.S.C. § 1028 (a) (7). Este delito, en la mayoría de las circunstancias, conlleva un plazo máximo de 15 años de prisión, una multa y el decomiso penal de cualquier bien personal utilizado o destinado a ser utilizado para cometer el delito.

Los esquemas para cometer robo de identidad o fraude también pueden involucrar violaciones de otras leyes como fraude de identificación (18 USC § 1028), fraude con tarjeta de crédito (18 USC § 1029), fraude informático (18 USC § 1030), fraude postal (18 USC § 1341), fraude electrónico (18 USC § 1343) o fraude de instituciones financieras (18 USC § 1344). Cada uno de estos delitos federales son delitos que conllevan penas sustanciales, en algunos casos, hasta 30 años de prisión, multas y confiscación criminal.

Los fiscales federales trabajan con agencias de investigación federales como el Buró Federal de Investigaciones, el Servicio Secreto de los Estados Unidos y el Servicio de Inspección Postal de los Estados Unidos para enjuiciar los casos de robo de identidad y fraude.

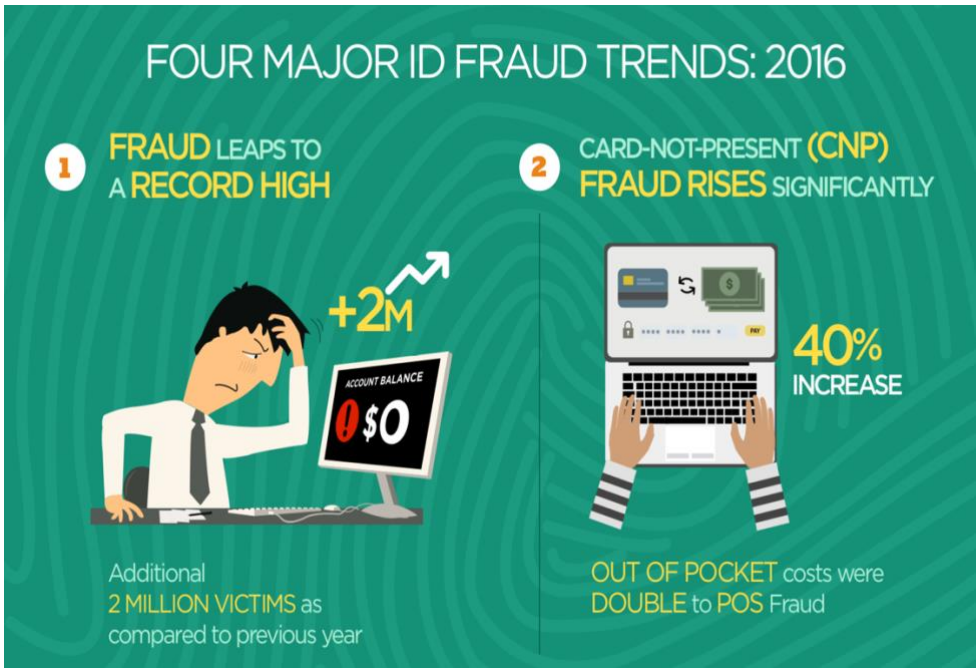
Según un estudio llevado a cabo por la empresa Javelin, el fraude de identidad alcanzó el récord más alto con 15.4 millones de víctimas estadounidenses en 2016, un 16 por ciento por arriba del anterior.

Los consumidores conectados digitalmente tienen un mayor riesgo de fraude de identidad, pero los consumidores fuera de línea tardan más en detectar el fraude.

[118] *Identity Theft and Assumption Deterrence Act*. En: https://www.ftc.gov/node/119459. Consultado el 11 de noviembre de 2016.

A continuación, presentamos una infografía elaborada por esta empresa[119]:

[119] ID Records Infographic. En: https://www.javelinstrategy.com/sites/default/files/17-1001J-2017-LL-Identity-Fraud-Hits-Record-Highs-Javelin.pdf. Consultado el 20 de marzo de 2017.


FOUR MAJOR ID FRAUD TRENDS: 2016
1
FRAUD LEAPS TO A RECORD HIGH
+2M
ACCOUNT BALANCE
$0
Additional 2 MILLION VICTIMS as compared to previous year
2
CARD-NOT-PRESENT (CNP) FRAUD RISES SIGNIFICANTLY
40% INCREASE
OUT OF POCKET costs were DOUBLE to POS Fraud


3
ACCOUNT TAKEOVER BOUNCES BACK
TOTAL ACCOUNT TAKEOVER (ATO) LOSSES
→ 2.3B, a 61% spike from previous year
→ VICTIMS PAYING an average of $263, which is 5 TIMES than average
4
NEW-ACCOUNT FRAUD (NAF) CONTINUES UNABATED
NAF victims DISCOVER FRAUD by reviewing their CREDIT REPORT
15%
CREDIT REPORT
DEBT
or when CONTACTED BY a DEBT COLLECTOR
13%

Sin pretender atemorizar, pero sí alertar a los usuarios de TIC, las estadísticas mostradas indican que el entorno informático presenta riesgos importantes para sus usuarios, los cuales irán muy seguramente en incremento, mostrando diversas mutaciones en la forma de comisión de los ilícitos.

En la legislación francesa, también se encuentra reconocida esta actividad ilícita, desde el año de 2005 la criminalidad ligada a los medios de identificación se convirtió en el común denominador de otros delitos.

Para el autor Guy de Felcourt, existen diferentes fenómenos que contribuyen al aumento de estos fraudes ligados a la identidad, uno de los más importantes: La ingeniería social,

entendida como el arte de la manipulación humana con la intención de llevar a cabo actividades fraudulentas o hacer revelar información confidencial o reservada a la víctima. Esta puede darse en línea o incluso vulnerando personalmente al individuo, que sin duda alguna es el eslabón más débil.

Como lo hemos postulado a lo largo de este trabajo, la usurpación de identidad no es una conducta novedosa, incluso podemos afirmar que se remonta a los propios orígenes del ser humano.

La identidad personal está ligada a fenómenos sociológicos y psicológicos, a la necesidad de ser reconocido, individualizado y estimado por el entorno social.

Históricamente la usurpación de identidad aparece desde las mitologías egipcia, griega y romana. Incluso, la palabra hipocresía, de origen griego, significa justamente fingir ser o sentir algo contrario a la realidad, el arte de la apariencia.

Si se ha retomado el tema con mucho mayor interés, es por las graves consecuencias económicas, y Francia no se ha escapado de estos efectos.

Apenas en 2015, el Observatorio Sociedad y Consumo, realizó un estudio acerca de la percepción de los ciudadanos franceses frente al tema de la usurpación de identidad y estos fueron los resultados:

La explotación de datos personales: una preocupación creciente ... especialmente para los datos digitales.

La explotación de datos personales es un tema cada vez más importante y una preocupación creciente para los franceses. El 66% de los encuestados dice que está preocupado por el uso malicioso que podría hacerse de sus datos personales. El 58% dice que ha aumentado su nivel de atención al compartir información personal con otros. Para más del 90% de ellos, es importante que las empresas o las administraciones eliminen su información personal después de su uso, y para más de la mitad de ellos, es "muy importante". Una expectativa que resulta en la eliminación de datos personales de las bases de datos digitales de las organizaciones, pero también en la destrucción sistemática de cualquier documento en papel que contenga información personal.

Sin embargo, es en el mundo digital donde se concentra la mayor parte de la atención de los individuos encuestados. Para el 96% de los encuestados que han aumentado su nivel de

cuidados y seguridad en línea, los datos proporcionados a través de Internet son objeto de especial atención, en comparación con solo el 30% de los documentos en papel.

Consistentemente, el 66% de los encuestados cree que existe un alto riesgo de que los datos que comunican en línea sean transmitidos o recibidos por terceros, especialmente en el caso de la compra en Internet o las suscripciones efectuadas en línea. Pero solo el 41% percibe un alto riesgo al transmitir documentos en papel.

En cuanto al modo de transmisión más riesgoso, el 4% de los encuestados opta por la transmisión física de documentos en papel, el 49% por Internet y el 42% percibe un riesgo equivalente. Cabe señalar, además, que la percepción del riesgo en lo que respecta a la transmisión de datos digitales es más preocupante para las generaciones más jóvenes.

Más y más información sensible en circulación

Sin embargo, si bien el desarrollo tecnológico ha incrementado el número de documentos digitales, no es seguro que este desarrollo vaya acompañado de una reducción efectiva en el número de documentos en papel que siguen existiendo en los hogares. De hecho, el 80% dice que imprime documentos digitales que contienen información personal, como contraseñas de correo electrónico o sitios de venta en línea. Sin embargo, estos documentos, menos "oficiales" que los documentos administrativos originales, son probablemente el tema de menor atención por parte de las personas, que en un 55% admiten no destruirlos sistemáticamente antes de tirarlas.

El estudio también revela una inflación de los intercambios de datos entre los hogares y las organizaciones, tanto en el dominio digital, pero no únicamente en este. Contrariamente a la creencia popular, la transmisión de documentos desmaterializados está lejos de haber dado lugar a una reducción en el número de documentos en papel enviados por los hogares a las empresas y las administraciones.

El 67% de los franceses dice que ha comunicado información personal a través de Internet a una organización al menos una vez en los últimos 12 meses (en comparación con el 50% en 2012). El 80% dice que ha proporcionado al menos una copia impresa de información personal a una organización en el último año (en comparación con el 75% en 2012). Este aumento está dando como resultado un volumen creciente de documentos que contienen información sensible en circulación. Entre ellos, los franceses otorgan la mayor importancia a los documentos administrativos y

financieros. Sin embargo, en la gran mayoría de los casos, estos documentos, al igual que otros documentos que contienen información personal, se guardan sin ninguna protección especiañ. El 35% también retiene algunos de sus documentos que ya no son útiles por falta de solución alternativa.

Robo de identidad: un riesgo importante para los franceses.

El 42% de los franceses considera que el robo de identidad es el riesgo más preocupante relacionado con la explotación y el uso malintencionado de los datos personales. Por lo tanto, ocupa la primera posición de los 7 tipos de riesgos propuestos, dado el riesgo de fraude con tarjetas de crédito (37%). La publicación de documentos o información confidencial sin su conocimiento, el riesgo de divulgación de las comunicaciones privadas o el uso comercial de los datos, que, aunque también forman parte significativa del muestreo, son menos relevantes.

Un miedo que se refleja en los comportamientos

Esta creciente preocupación de las personas sobre el mal uso de sus datos personales ahora se ve reflejada en su comportamiento. El 76% de los franceses ya se ha negado a comunicar información personal a través de Internet y el 37% ha transmitido documentos en papel para protegerse de los riesgos del uso ilegal de sus datos. El 52% habría renunciado a una compra por no tener que revelar información en Internet y el 42% no aceptaría proporcionar documentos en papel que contengan información confidencial.

Sin embargo, de acuerdo con la percepción general, observamos estrategias de autoprotección mucho más desarrolladas en el mundo digital que para los documentos en papel. Mientras que casi tres cuartas partes de los encuestados dicen que se han negado a proporcionar información personal a través de Internet, por ejemplo, sólo la mitad de las personas se niegan a enviar documentos en papel que contienen información personal. Del mismo modo, mientras que el 31% de los franceses dicen que ya han comunicado información falsa a una organización a través de Internet, esta proporción solo alcanza el 18% cuando se transmiten documentos en papel.

El francés, sin embargo, reacciona de forma unánime en este punto: quiere la destrucción de documentos que contengan datos personales después de su uso por las organizaciones responsables de los mismos (91% para el papel / 93% para los datos almacenados en bases de datos digitales recabados en línea).

El robo de identidad está directamente relacionado con lo que se conoce como crimen documental y de identidad, que incluye delitos que afectan la identidad de las personas y las empresas. A diferencia de la creación de una identidad falsa, la sustitución de identidad (intercambio de identidad voluntario y simétrico) o el robo de identidad, la usurpación de la identidad lleva a la víctima a tener que demostrar que ella es inocente. Sus consecuencias morales, financieras y sociales a menudo son desastrosas para las víctimas, pero a menudo son ignoradas.

Los daños asociados con el robo de identidad pueden ser numerosos. En cuanto a la comisión de delitos, la víctima puede terminar siendo despojada de su propiedad, ser procesado penalmente por actos que no cometió, etc., sin embargo, se observó con mayor frecuencia daños y afectaciones de carácter civil, por ejemplo, sin saberlo, la víctima puede llegar a casarse (por lo general permite que el usurpador obtener la naturalización) o incluso ser reconocido jurídicamente como "padre" de niños que ni siquiera conoce, casos donde cara al Banco de Francia, una persona sea declarada muerta para cobrar un seguro de vida, etc. En estos casos, además, la víctima enfrenta la imposibilidad de encontrar trabajo y, sobre todo, la incapacidad de demostrar su propia identidad ante las autoridades.

En 2014, se observa la estabilidad relativa de los datos sobre los delitos relacionados con la identidad (Fuente: NPD, DCPJ / PTS - PAFISA Archivo - INHESJ / ONDRP - Agosto 2015):

- 119,023 personas que usan al menos una identidad falsa;
- 11,739 delincuentes acusados;
- 14,060 hechos registrados.

Sin embargo, estas cifras solo reflejan la actividad policial, no la realidad del fenómeno criminal. Por un lado, los delitos que afectan la identidad están destinados por naturaleza a ocultarse, y en el caso de un delito relacionado, se consideran secundarios. Por otro lado, los delitos descubiertos en el extranjero no se registran en las estadísticas francesas. Sin mencionar que este delito se reconoce como tal en la legislación francesa a partir de marzo de 2011, y que el 80% de las víctimas desconocen que son víctimas en el momento y presentan una queja en promedio dos años después del incidente.

Desde el punto de vista operativo, si los documentos de identidad centrales (tarjeta de identidad, pasaporte, licencia de conducir) fueron anteriormente los más codiciados y los más

fraudulentos, ahora los son las copias de actas de nacimiento, copias de nóminas, documentos de identidad o facturas. De 30 millones de tarjetas de identidad en Francia, se estima que aproximadamente el 10% de ellas es "cuestionable".

La mayoría de las personas cree que la suplantación de identidad se realiza con mayor frecuencia a través de Internet, mientras que las denuncias de robo de identidad mediante piratería actualmente representan un porcentaje insignificante. De los 14,060 casos oficiales, el 99% se refiere al robo de identidad realizado con documentos en papel o copias de documentos. Sin embargo, este riesgo existe y no debe descuidarse, especialmente porque va en aumento a una velocidad impresionante. El robo de datos está aumentando drásticamente en el ciberespacio, y controlar el uso de los datos personales y destruirlos se hará cada vez más difícil con la popularización del cómputo en la nube.

En Francia, antes del 2011, la usurpación de identidad no constituida un delito en sí mismo, ahora el Código Penal, como fruto de la creación de la Ley n° 2011-267 del 14 de marzo 2011 de Orientación y de Programación para la mejora de la Seguridad Interior, mejor conocida como LOPSI.

El Artículo 226-4-1 dispone que:

> *"El hecho de suplantar a un tercero o el uso de uno o más datos de cualquier naturaleza, que permitan identificarlo con el fin de perturbar su tranquilidad o la de otro, o atentar contra su honor o su consideración, se castiga con un año de prisión y una multa de € 15,000.*
>
> *Este delito se castiga con las mismas sanciones cuando se comete en una red de comunicación al público, en línea."*

CAPÍTULO II: IDENTIDAD DIGITAL Y DERECHO ADMINISTRATIVO.

A la fecha, las autoridades de carácter administrativo, son las que han tomado a su cargo la puesta en marcha de medias disuasivas, preventivas, informativas y de contención, para tratar

de frenar el fenómeno de la usurpación de identidad.

Como ya vimos en los capítulos anteriores, en el caso de Francia, es la CNIL la que se ha encargado de hacer recomendaciones al ciudadano respecto de cómo prevenir, y en su caso hacer frente a este tipo de actividades ilícitas.

Es posible también generar una denuncia en línea de manera anticipada, conocida como pre-denuncia.

https://www.pre-plainte-en-ligne.gouv.fr

En el caso de Estados Unidos, como ya explicamos anteriormente, es la FTC a quien se remiten las quejas a través del sitio de Internet: https://www.identitytheft.gov.

En México, las autoridades de carácter administrativo también se han dado a la tarea de generar comunicaciones al público y advertencias tendientes a prevenir estos casos, a continuación, se muestran las alternativas que han presentado:

- CONDUSEF:
  - http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad
  - http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/655-ante-el-robo-de-identidad
  - http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos/307-protege-tu-identidad
  - https://www.gob.mx/condusef/acciones-y-programas/robo-de-identidad

- PROFECO:
  - https://www.gob.mx/cms/uploads/attachment/file/95761/CONDUGUIAS-ROBODEIDENTIDAD.pdf

- INAI:

- https://www.gob.mx/cms/uploads/attachment/file/95761/CONDUGUIAS-ROBODEIDENTIDAD.pdf

CAPÍTULO III: IDENTIDAD DIGITAL Y DERECHO CIVIL.

Hemos hablado ya de los derechos de la personalidad y el reconocimiento del Derecho Civil moderno, que se hace frente aquellos bienes morales, dentro de este reconocimiento encontramos la figura del daño moral.

Por daño se entiende cualquier pérdida o menoscabo, deterioro, ofensa o dolor que se provoca a una persona, cosa o valores, de los que alguien es titular.

En este sentido, cuando algún bien es vulnerado, esta lesión no solamente implica aspectos económicos sino también de índole moral, como los casos que hemos explicado anteriormente, donde la víctima sufre daños psicológicos y emocionales, en muchos casos irreparables, ya que el daño trastoca aspectos tan íntimos como la dignidad, la integridad o la propia imagen.

En este orden de ideas, surge la necesidad de instituir una figura que permita indemnizar o reparar de alguna forma el daño sufrido en los bienes económicos o morales de las víctimas.

El daño moral es una acción de carácter civil, reconocida por las tres legislaciones analizadas en este trabajo. El derecho francés es pionero en la materia, seguido del derecho anglosajón y el derecho mexicano.

Así que el derecho civil, entra en acción cuando por alguna violación a la identidad, a la vida privada o a los datos personales, la víctima sufre algún tipo de daño ya sea de carácter económico o moral, en busca de una posible reparación.

El ejercicio de esta acción sigue diferentes criterios dependiendo de cada uno de los países.

En Francia [120], para llevar a cabo el reclamo de indemnización, debe constituirse

[120] La responsabilité extracontractuelle en général. En : https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721&idSectionTA=LEGISCTA000032

debidamente un expediente, la víctima debe establecer la evaluación del monto de la reparación (incluidos los costos directamente relacionados con el daño sufrido).

La víctima también debe probar lo siguiente:

- Que el daño o lesión fue causada por un hecho específico y determinado.
- La persona a quien busca reparación es responsable de su lesión,
- El daño es real, directo y le concierne personalmente,
- El daño o perjuicio, ya sea presente o futuro, puede ser objetivamente determinado y evaluado.

La víctima presenta un reclamo destinado a compensar todos los daños sufridos. El juez no puede ordenar que el demandado pague más allá del monto de reclamo de la víctima.

Ella debe presentar evidencia de su lesión.

La víctima puede apelar ante un tribunal civil ya sea que la persona responsable del daño haya cometido un delito o no. El tribunal competente depende del tipo y la cantidad de la disputa.

El tribunal competente depende de las sumas involucradas en la disputa.

- Para una disputa de menos de € 10,000, es el tribunal de distrito (TI).
- Para una disputa por encima de € 10,000, es el Tribunal de Grande Instance (TGI).
- La víctima también puede pedirle al juez que imponga una multa. Si se impone la multa, el responsable de la indemnización está obligado a pagar una cantidad adicional de dinero por retraso en el pago.

La legislación estadounidense que toma como antecedente al derecho francés, por lo tanto está basada en criterios similares, sin embargo, en la práctica podemos observar que hay casos donde se demandan cantidades exorbitantes de dinero basados en hechos y razonamientos no siempre

021488 Consultado el 12 de noviembre de 2017.

objetivos.

Cuando una lesión resulta de una acción negligente o maliciosa de una persona a otra persona, la persona que sufrió la lesión puede reclamar daños en forma de compensación monetaria. El jurado o juez ejerce un amplio poder discrecional para otorgar daños compensatorios en asuntos de daños morales. La medida de los daños compensatorios debe ser real y tangible. Es difícil fijar una cantidad con certeza en casos que involucran reclamos como dolor y sufrimiento o angustia emocional. Al evaluar el monto de los daños compensatorios que se otorgarán, el juez o el jurado deben ejercer el buen juicio y el sentido común, sobre la base de la experiencia general y el conocimiento de economía y el entorno social. Sin embargo, una adjudicación apropiada estaría basada en la evidencia sustancial.

El dolor y el sufrimiento son un elemento adecuado para recuperar la compensación monetaria por daños causados por un acto negligente o una omisión. Cuando la exigencia de la compensación se basa en la angustia mental, el juez o el jurado se basa en elementos tales como:

- Las circunstancias totales que rodean el incidente, y
- La credibilidad de las pruebas sustanciales y los testigos.

Cualquier demandante tiene derecho a una indemnización por el dolor y el sufrimiento sufrido como consecuencia de un hecho ilícito u omisión. El dolor y el sufrimiento también incluyen el sufrimiento que la persona sufrió durante cualquier cirugía o tratamiento médico que razonablemente fuera consecuencia del hecho ilícito.

Bajo la categoría de "dolor y sufrimiento", un demandante puede reclamar daños incluso por miedo, nerviosismo, dolor, ansiedad, preocupación, mortificación, conmoción, humillación, atentados a su dignidad, vergüenza o terror. El dolor y el sufrimiento también incluyen desfiguración y deformidad, deterioro de la capacidad para trabajar, ansiedad o preocupación atribuibles a una lesión y angustia mental causada por el hecho ilícito. Sin embargo, no se pueden otorgar daños por dolor y sufrimiento si no hay pruebas de lesiones graves o si existen pruebas suficientes para acreditar que el dolor solo es imaginario.

El jurado debe estar convencido sin lugar a dudas de que el demandante sufrió dolor antes de permitir una compensación por el dolor. La cuestión del dolor y el sufrimiento debe ser

resuelta por la conciencia imparcial y el juicio de los miembros del jurado que se espera que actúen de manera razonable, inteligente y en armonía con la evidencia.

La regla general es que cuando se aplican daños especiales a un caso, también se deben otorgar daños generales. Donde no hay dolor inmediato o sustancial, no es necesario otorgar daños por el dolor y el sufrimiento. Un jurado puede denegar una compensación por dolor y sufrimiento a pesar de que el demandante incurrió en una pérdida de salarios y gastos médicos, si la evidencia de la lesión del demandante es subjetiva. No hay un estándar específico que se debe seguir para determinar la cantidad exacta como daños por el dolor y el sufrimiento. Sin embargo se espera que el poder discrecional proporcionado al jurado no se ejerza de manera abusiva.

Cuando el dolor y el sufrimiento fueran consecuencia de un accidente, el dolor y el sufrimiento futuro de la persona lesionada constituirán un elemento apropiado para solicitar los daños morales. En este caso de debe comprobar al menos la probabilidad de que el futuro dolor y sufrimiento resulten del accidente. Incluso si la lesión no es permanente, se le puede permitir al demandante acreditar un dolor y sufrimiento futuro solo si demuestra que su dolor y sufrimiento es cierto y puede continuar por un período prolongado.

Un jurado puede otorgar la compensación bajo su poder discrecional a una persona angustiada emocionalmente si es evidente que la angustia mental fue causada como resultado del accidente.

Los jueces y los jurados confían en el dolor físico y el sufrimiento mental, así como en muchos otros factores relevantes para determinar la cantidad de daños en una acción de esta naturaleza. La determinación completamente precisa de la cantidad no es posible en tales casos. No hay una regla estándar para medir los daños. El jurado puede decidir sobre el asunto utilizando su poder discrecional. Los tribunales solo pueden interferir en los casos en que exista un claro abuso de esta discreción. Los jurados en su mayoría determinan el monto con base a estándares justos y razonables, libres de estándares sentimentales o caprichosos y basados en la evidencia provista. Los daños otorgados deben ser proporcionales a la lesión sufrida. El jurado debe considerar la naturaleza y el alcance de las lesiones, el dolor resultante y la duración durante la cual la persona sufrió el dolor de la lesión.

El jurado también debe considerar la edad, los hábitos de salud y el estado de la

parte afectada antes y después de la lesión. El juez o el jurado también consideran la necesidad de tratamiento médico, psicológico o psiquiátrico, la presencia de síntomas físicos, la pérdida de ingresos y el impacto en la conducta y el estilo de vida del demandante antes de prorratear el monto de los daños.

El uso de sedantes y drogas para aliviar a los heridos del dolor también es evidencia prominente para mostrar la gravedad del dolor y el sufrimiento. Los heridos también tienen que vivir bajo un costo de vida aumentado cuando la persona pierde la capacidad de ganar dinero. Este factor también ayuda al jurado a determinar el alcance de los daños que se otorgarán.

En México, la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal, establece los medios de defensa del derecho a la vida, al honor y a la propia imagen.

> *"Artículo 35.- La tramitación de la acción se sujetará a los plazos y condiciones establecidos para los procedimientos en Vía de Controversia en el Código de Procedimientos Civiles para el Distrito Federal.*
>
> *Artículo 36.- Para que se produzca el daño al patrimonio moral se requiere:*
>
> *I.- Que exista afectación en la persona, de los bienes tutelados en la presente ley;*
>
> *II.- Que esa afectación sea a consecuencia de un acto ilícito; y*
>
> *III.- Que haya una relación de causa-efecto entre ambos acontecimientos.*
>
> *Para la procedencia de la acción se deberá tomar en*

cuenta la mayor o menor divulgación que el hecho lesivo ha tenido, las condiciones personales de la víctima y las demás circunstancias del caso.

Artículo 37.- La carga de la prueba recaerá, en principio sobre el actor, quien deberá demostrar el daño en su derecho de personalidad derivado de un hecho ilícito.

La valoración del daño al patrimonio moral debe ser realizada tomando en cuenta la personalidad de la víctima, su edad, posición socioeconómica y naturaleza pública o privada, la índole del hecho ilícito, la gravedad objetiva del perjuicio, la mayor o menor divulgación.

Artículo 38.- Las acciones para exigir la reparación del daño contenidas en la presente ley prescribirán a los dos años de la fecha en que se causó efectivamente el daño que contará a partir de la realización del acto que se presume ilícito.

Articulo 39.- La reparación del daño comprende la publicación o divulgación de la sentencia condenatoria, a costa del demandado, en el medio y formato donde fueron difundidos los hechos y/u opiniones que constituyeron la afectación al patrimonio moral.

Artículo 40.- En ningún caso, las sanciones derivadas del daño al patrimonio moral serán privativas de la libertad de las personas.

Artículo 41.- En los casos en que no se pudiere resarcir el daño en términos del artículo 39 se fijará indemnización tomando en cuenta la mayor o menor divulgación que el acto ilícito hubiere tenido, las condiciones personales de la víctima y las demás circunstancias del caso, en ningún caso el monto por indemnización deberá exceder de trescientos cincuenta días de salario mínimo general vigente en el Distrito Federal, lo anterior no incluye los gastos y costas que deberá sufragar y que podrán ser restituidos conforme lo que dispone en estos casos el Código Procedimientos Civiles para el Distrito

Federal.

En los casos de los sujetos contemplados en el artículo 33 de esta ley el Juez podrá, dependiendo las características especiales del caso, disminuir hasta en un setenta por ciento la cantidad máxima establecida en el presente artículo.

Artículo 42.- Mientras no sea ejecutoriada la sentencia no se tendrá por totalmente concluido el expediente. El juez podrá dictar las medidas de apremio que la ley le autorice para el debido cumplimiento de la sanción.

Artículo 43.- En caso de reincidencia, en el plazo de un año, el Juez podrá imponer hasta en una mitad más del monto máximo por indemnización.

Artículo 44.- Las resoluciones derivadas por el la acción de daño moral podrán ser impugnadas conforme a los procedimientos y plazos que establece el Código de Procedimientos Civiles para el Distrito Federal.

CONCLUSIÓN DE LA SEGUNDA PARTE.

La Sociedad de la Información y la forma en la que nos desempeñamos en ella, ha significado una serie de retos legislativos para los países y las autoridades que tienen que hacer frente a nuevas formas de comisión de ilícitos ya sean de carácter penal, administrativo o civil; hay que convertirse un poco en mago para poder hacer frente a estos desafíos legales agotando todas las instancias existentes, la vía penal no siempre es la idónea ni la más sencilla, es momento de entender a la protección de la identidad digital como un aparato jurídico holístico que tendrá que echar mano de las diferentes ramas del derecho para salvaguardar los derechos de la víctima y resarcir el daño en la medida de lo posible.

TERCERA PARTE: IDENTIDAD DIGITAL COMO FUENTE DE EVOLUCIÓN DEL DERECHO

CAPÍTULO I: LA EVOLUCIÓN DE LA TUTELA DE LA IDENTIDAD DIGITAL COMO UN CONJUNTO DE DATOS PERSONALES.

Hemos abordado el tema de la personalidad y dentro de ese mundo, desprendido la identidad o, mejor dicho, el conjunto de identificadores que permiten a una persona estar presente el mundo, hacer su vida diaria y su rutina, ahora tocaremos de forma más precisa y contundente el tema de la identidad digital.

Asimismo, se ha realizado un esfuerzo de conceptualización de identidad digital, para tales efectos, entenderemos a la identidad digital como el conjunto de elementos de identificación que sirven a una persona física, moral o entidades gubernamentales, para distinguirse de otras en un entorno digital o virtual, ya sea para construir una reputación digital, para comunicarse, relacionarse, adquirir derechos y obligaciones con otros usuarios o únicamente para tener visibilidad en los medios informáticos.

La identidad digital es una paradoja de elementos que pueden a su vez servir como identificadores y herramientas para aninimizar; es decir, que mientras algunas personas físicas o morales aprovechan estos elementos de individualización para ser reconocidas como tal, o bien, trasladar su identidad real o corporativa a un entorno digital, otras personas, sobre todo físicas, aprovecharan estos elementos para distraerlos de su identidad habitual y de alguna manera gozar de un cierto nivel de anonimato.

Existe un cúmulo de personas físicas que generan un avatar que refleja su alter ego, pero que al no revelar de inicio su verdadera identidad, les permite desempeñarse con mayor soltura en los medios digitales.

Personas que desempeñan un cargo importante en una empresa, políticamente expuestas, jefes de gobierno, clérigos o simplemente personas tímidas, o cuya integridad física se encontraría en peligro en caso de revelar su nombre, utilizan estos avatares para poder expresarse libremente; sin embargo, también dentro de este grupo de personas interesadas en gozar del anonimato, podemos encontrar cibercriminales.

Tal y como lo relata Alain Bobant en el prefacio del libro intitulado, Internet y las Redes sociales, desde el 2005, el internauta ha comenzado a explotar comportamientos inéditos adoptando la "*Web attitude*", aislado pero desinhibido, se nuestra, se da a conocer, se expresa, se exterioriza, se singulariza, se destaca, se ilustra, influye… Pero al mismo tiempo al interactuar y exhibirse, se expone a riesgos de toda naturaleza.

La e-reputación, es un concepto que tiene una naturaleza sociológica pero también mercadológica, a lo largo de nuestro paso por Internet y todas las plataformas sociales que viven en esta gran red, vamos dejando huella, una huella por desgracia, prácticamente imborrable, que puede dejar antecedente de todos nuestros éxitos laborales, pero también de errores del pasado, fotografías poco afortunadas, amistades no gratas, etc.

La complejidad más grande que representa la e-reputación, es que se basa no sólo en lo que nosotros podemos decir o mostrar de nosotros mismo, de nuestra vida o de nuestra carrera, sino que también se construye de las opiniones, fotografías, videos y recuerdos de los demás, esos cohabitantes del ciberespacio que no siempre son nuestros amigos o familia, a veces son nuestros maestros, alumnos, colegas, clientes o incluso detractores.

La importancia de la e- reputación o reputación en línea, es tanta, que al día de hoy existen empresas que se dedican a vender servicios de limpieza de reputación en línea, una de estas empresas es precisamente un startup francés llamada SOS reputation[121], que ofrece "limpiar" la imagen de las personas o empresas, claro, no se trate de borrar los antecedentes negativos, sino de "ocultarlos".

En el año de 2014, la autora, acudió a suplir a un profesor a su clase, al momento de llegar al aula, sin haberme presentado, le solicité a los alumnos que descubrieran algunos elemento de mi identidad y para ello tendrían tan sólo cinco minutos, por lo menos tendrían que encontrar mi nombre, y la única pista que tenían era el nombre del profesor titular de la materia; al terminar ese lapso, el 90% de los alumnos, es decir, treinta y cinco alumnos, pudieron decirme mi nombre completo, el nombre de la empresa donde trabajo, mi usuario de Twitter y el nombre de la escuela donde había estudiado la maestría; no es casualidad, se llama teoría de grafos[122] o teoría de gráficas.

[121] SOS reputation. En: http://www.sos-reputation.com/es/
[122] García Miranda, Jesús, *Introducción a la Teoría de Grafos*. En: http://www.ugr.es/~jesusgm/Curso%202005-2006/Matematica%20Discreta/Grafos.pdf. Consultado el 20 de diciembre de 2015.

Esta teoría es un principio matemático que data de 1736, un grafo, es una estructura matemática que permite modelar problemas de la vida cotidiana, mediante, como hemos visto, una representación gráfica formada por nodos o vértices que muestra a los actores y aristas que sirven para representar los lazos o relaciones entre los actores. Así mismo, un grafo puede representar un único tipo de relación entre los actores (simple), o más de un tipo de relación (múltiple), además cada vínculo o relación puede ser orientado[123].

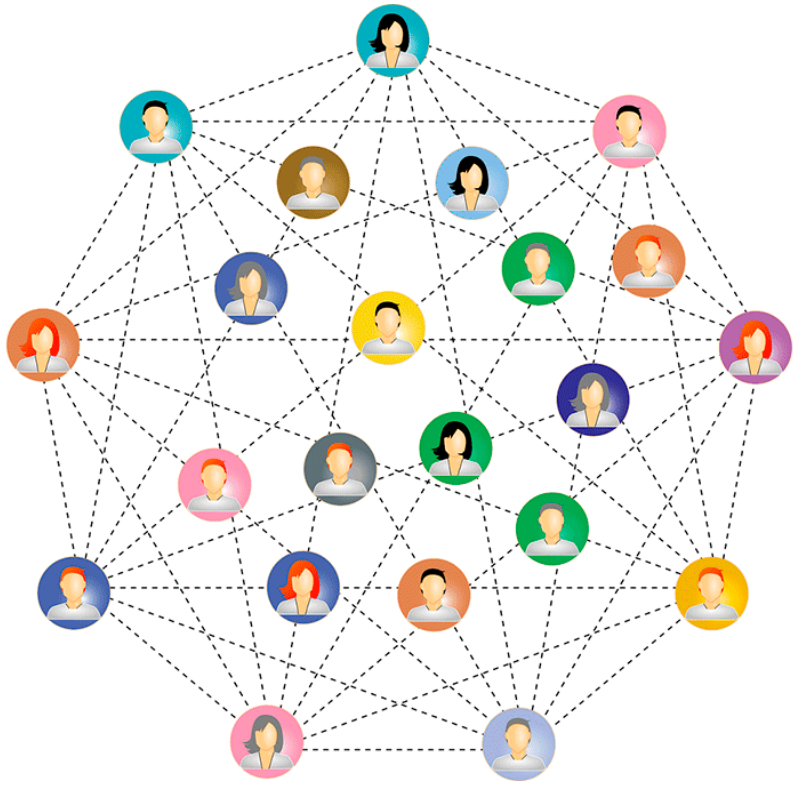


Fig. 12 Expresión de la teoría de grafos para ejemplificar el funcionamiento de las redes sociales[124]

La e-reputación es algo tan importante hoy en día, que muchos de los reclutadores a nivel mundial consultan información de sus candidatos, o incluso, encuentran a sus candidatos a través de redes sociales, si bien, el Código Laboral francés prohíbe expresamente recabar datos de los candidatos o empleados de su "entorno privado", esto no significa que sea una práctica común, en

[123] Rochina, Paula, *El análisis de redes sociales mediante la teoría de grafos.* En: https://revistadigital.inesem.es/informatica-y-tics/teoria-grafos/. Consultado el 10 de mayo de 2017.
[124] *Ibidem*

Estados Unidos o en México, no es una actividad regulada, por lo que estimamos que al menos el 70% de las empresas de reclutamiento utiliza redes sociales para encontrar a sus recursos humanos, o peor aún, para "evaluarlos", incluso a nivel psicológico o comportamental[125].

Desde luego que esto podría abrir un gran debate respecto del cúmulo de derechos fundamentales que se violan al hacer este tipo de consultas, entre ellos: el derecho a la privacidad, a la protección de los datos personales y a la no discriminación entre otros, sin embargo, esto no significa que no sea una práctica común.

El ser humano comienza a interactuar en un universo que consideramos aun no dimensiona correctamente, el universo de la Internet.

Internet, concebido en un inicio como un servicio de telecomunicaciones e intercambio de información que hoy en día llega a nuestros hogares gracias a los prestadores de servicios de Internet (PSI, ISP por sus siglas en inglés y FAI por sus siglas en francés), y que se ha convertido en un mundo alterno donde nos mudamos a desempeñar una gran cantidad de actividades de nuestro día a día, desde consultar el diario de la mañana hasta trabajar, buscar documentacion, acceder a música, libros y videos de todo el mundo, estudiar a distancia, ir al banco, hacer las compras de la casa, convivir con nuestros amigos, familia, completos desconocidos, convocar movimientos sociales, hasta inventarnos una vida ficticia.

El contenido de la información a la que podamos acceder en Internet, dependerá de la calidad de los servicios prestados por los prestadores, tal como lo reconoce la corte de alzada de París en 2014, los PSI, pueden ofrecer contenidos exclusivos y servicios innovadores exclusivos para aumentar su cartera de manera completamente lícita.

Uno de los grandes problemas de la actividad humana en Internet, tiene que ver precisamente con los limites casi imperceptibles, grises y tenues, ¿Acaso en pro de la libertad de expresión es que podemos decir lo que sea en Internet?, ¿Cuáles son las reglas que guían nuestra actividad y las normas aplicables?

[125] Tus redes sociales: a examen de los reclutadores, El Financiero. En: http://www.elfinanciero.com.mx/power-tools/tus-redes-sociales-a-examen-de-los-reclutadores.html. Consultado el 17 de noviembre de 2017.

Gracias a los motores de búsqueda y otros robots, la identificación y la trazabilidad de los comportamientos son consustanciales a las redes digitales. Este seguimiento prohíbe cualquier confidencialidad real de las comunicaciones. Limita la impunidad frecuente de ciertos comportamientos en el mundo real e incluso socava el "derecho al olvido". El resultado es una paradoja obvia: la facilidad, la gratuidad y la inmediatez de la comunicación digital que conducen a prácticas individuales y colectivas desacreditadoras (y a veces reprensibles en el sentido legal), especialmente en las redes sociales, deben ponerse en perspectiva con la fácil identificación de estas prácticas. Hay una banalización del comportamiento combinada con un aumento en el riesgo legal[126].

Así como los derechos nacen a partir de las obligaciones, la libertad no es absoluta, tiene límites marcados por el bien común y los derechos de terceros. La libertad de expresión nacida en Francia con la revolución, luego de la proclamación de la Declaración de los Derechos del Hombre y el Ciudadano de 1789, los artículos 10 y 11, prevén que por una parte nadie debe ser molestado o incomodado por la expresión de sus opiniones inclusive las religiosas a no ser que afecten el orden público establecido por la Ley y por la otra; la libre comunicación de sus opiniones y pensamientos es uno de los derechos más preciados del hombre, por lo tanto, todo ciudadano puede hablar, escribir e imprimir libremente, salvo aquellos casos previstos por la Ley en los que tenga que responder por el abuso de esta libertad.

La ley francesa del 30 de septiembre de 1986 relativa a la libertad de comunicación, precisa que, específicamente en lo que respecta a la expresión en Internet: “la comunicación por vía electrónica es libre. El ejercicio de esta libertad no puede ser limitado que en la medida requerida, por una parte por el respeto de la dignidad de la persona humana, de la libertad y la propiedad de un tercero, del carácter pluralista de la expresión de las corrientes de pensamiento y opinión, y por otra parte, la salvaguarda del orden público en atención a la necesidad de de la defensa nacional.

A efecto de comprender lo que se entiende por “comunicación pública por vía electrónica”, en términos de la citada Ley como: “Toda puesta a disposición del público o categorías de público, mediante un proceso de comunicación electrónica, signos, señales, escritos, imágenes, sonidos o mensajes de cualquier naturaleza que no tengan el carácter de correspondencia privada”.

[126] Latreille, Antoine, *Numérisation*, (2017) 22 Lex electronica 117. En : http://www.lex-electronica.org/en/s/1567. Consultado el 9 de diciembre de 2017.

Luego entonces, el internauta goza de una libertad de expresión plenamente reconocida para poder expresarse en línea, ya sea en un blog, en una red socia, en un foro de discusión, etc, con los límites establecidos por la Ley, principalmente aquellos ligados a la dignidad, el honor y al respeto a la vida privada.

En Estados Unidos, la Ley presenta diferencias sustanciales, la primera enmienda de la Constitución de los Estados Unidos, adoptada en 1791, prohíbe toda restricción a la libertad religiosa, a la libertad de expresión y a la libertad de prensa.

La Constitución Política de los Estados Unidos Mexicanos, que es de una tradición más apegada al espíritu de la legislación europea que a la tradición norteamericana, reconoce también el derecho a la libertad de expresión y a la libertad de prensa, con el límite claro de la afectación a terceros, a la prescribe:

> *"…Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.*
>
> *Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión…"*

Complementándose con el:

> *"…Artículo 7o. Es inviolable la libertad de difundir opiniones, información e ideas, a través de cualquier medio. No se puede restringir este derecho por vías o medios indirectos, tales como el abuso de controles oficiales o particulares, de papel para periódicos, de frecuencias radioeléctricas o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios y tecnologías de la información y comunicación encaminados a impedir la transmisión y circulación de ideas y opiniones.*

Ninguna ley ni autoridad puede establecer la previa censura, ni coartar la libertad de difusión, que no tiene más límites que los previstos en el primer párrafo del artículo 6o. de esta Constitución. En ningún caso podrán secuestrarse los bienes utilizados para la difusión de información, opiniones e ideas, como instrumento del delito."

En la vida real, ante un litigio, los usuarios de una red social como Facebook, cara a la legislación aplicable por contrato, es decir, la de California, Estados Unidos, tendrían libertad plena para poder expresarse, aunque esta expresión violara ciertos límites reconocidos por las leyes francesas y mexicanas; sin embargo, el 5 de marzo de 2015, el tribunal de Gran Instancia de París, se estimó como competente para juzgar el comportamiento de un usuario de Facebook, y de igual manera, si una conducta fuera violatoria de los derechos de los mexicanos, aún y cuando sea expresada a través de una red social establecida en Estados Unidos, las autoridades mexicanas están en facultad de atraer el caso a su jurisdicción en los diferentes ámbitos de sus competencias.

Es claro entonces, que a la libertad de expresión le son aplicables los límites impuestos por los derechos de terceros y el orden público sin importar la jurisdicción contractual, tal es el caso de la condena a Google que le impuso el Tribunal de Gran Instancia de París el 6 de noviembre del año 2013, para que dejara de publicar fotos de la vida sexual de un dirigente de competencias de autos; así como muchos otros, incluyendo desde luego los casos de Derecho al olvido en Europa y México, uno de ellos precisamente contra Google.

Además de los riesgos que implica la interacción en Internet para la vida privada, también es importante recalcar algunos otros, como el caso de los delitos en contra del honor, por desgracia, estos delitos fueron derogados de los códigos penales mexicanos gradualmente desde el año 2007, en el caso de Francia, la Ley del 29 de julio de 1881 sobre la libertad de prensa, precisa las reglas que debe respetar toda clase de publicación, incluyendo desde luego aquellas efectuadas a través de Internet, asimismo, en su artículo 29 define lo que se entiende por difamación: "Toda alegación o imputación de un hecho que atente al honor o a la consideración de la persona o del cuerpo al que el hecho ha sido imputado, es una difamación. La publicación directa o por vía de reproducción de dicha alegación o imputación es punible aun si esta fue planteada en forma dubitativa o si ataca a una persona o cuerpo no expresamente identificada pero cuya identificación es posible".

En México y Estados Unidos, se prevén acciones civiles a modo de resarcimiento de daños morales.

El tema se torna muy interesante frente al potencial riesgo de ver nuestra imagen y reputación digital afectada por algún tipo de difamación a través de una red social, existen algunas redes sociales que son más propensas a estas situaciones ilícitas como es el caso de Twitter, Facebook o Instagram, pero más aún Twitter, ya que las personas pueden sin ninguna limitación previa, afirmar hechos o circunstancias falsas que puedan suponer un daño moral o económico a la persona física o moral difamada.

El 26 de julio de 2011, el Tribunal de Comercio de París, condenó al dirigente de una empresa al pago de 10,000 euros por concepto de daños y perjuicios a un prestador de servicios denigrando a este último a través de la red social Twitter.

Ahora bien, la persona acusada de difamación puede ser exculpada si prueba fehacientemente que los hechos que afirma son verdaderos, siempre y cuando no se trate de circunstancias que competen a la vida privada de la persona afectada.

En el caso la normativa mexicana, existe contamos con la Ley Reglamentaria del Artículo 6o., párrafo primero, de la Constitución Política de los Estados Unidos Mexicanos, en Materia del Derecho de Réplica, que como su nombre lo indica, establece los parámetros para ejercer el derecho de réplica que según el artículo 2º de la citada Ley, consiste en:

> *"... II. Derecho de réplica: El derecho de toda persona a que sean publicadas o difundidas las aclaraciones que resulten pertinentes, respecto de datos o informaciones transmitidas o publicadas por los sujetos obligados, relacionados con hechos que le aludan, que sean inexactos o falsos, cuya divulgación le cause un agravio ya sea político, económico, en su honor, vida privada y/o imagen..."*

Y es directamente aplicable a la prensa o a cualquier medio de comunicación, entendiendo por éste:

> *"... III. Medio de comunicación: La persona, física o moral, que presta servicios de radiodifusión; servicios de televisión o audio restringidos; o que*

de manera impresa y/o electrónica difunde masivamente ideas, pensamientos, opiniones, creencias e informaciones de toda índole y que opera con sujeción a las disposiciones legales aplicables."

Y por extensión a productores independientes:

"... IV. Productor independiente: La persona, física o moral, que genere y sea responsable de producir contenidos que sean publicados o transmitidos por los medios de comunicación."

Es decir, que las disposiciones de esta Ley son perfectamente aplicables al mundo virtual, tato sitios web, diarios y *blogs,como* redes sociales en línea y plataformas de contenidos audiovisuales, como *Youtube*, *Facebook*, *Instagram*, *Vimeo*, *Twitter*, *Blogger*, *Wordpress*, etc.

En este caso el afectado tiene un plazo de cinco días hábiles para enviar su escrito de petición directamente al medio de comunicación, agencia de noticias o productor independiente y en caso de omisión injustificada de respuesta por parte de éstos últimos; podrá ser llevado directamente el procedimiento ante un juez de distrito.

La legislación francesa también prevé un procedimiento similar en la Ley de 1881, respecto de las personas nombradas en algún diario o escrito periodístico, pero en lo que concierne de manera directa a publicaciones efectuadas a través de la Internet, la norma aplicable es la Ley de 2004 para la Confianza en la Economía Digital (LCEN, por sus siglas en francés), en términos del artículo 6-IV. El plazo para ejercer este derecho es de tres meses a partir de la publicación.

Cabe destacar que la citada Ley, si bien toca diferentes temas relacionados con el comercio electrónico uno de sus principales ejes es la protección de los datos personales.

Ahora bien, las circunstancias para la defensa del Derecho al Honor, a la protección de los datos personales y a la vida privada se complican luego de que se encuentra de por medio el anonimato, ya sea que el titular del sitio web donde fue publicado el comentario o la información difamatoria no sea fácilmente rastreable, o bien, porque el usuario en lo particular, que a través de un sitio web o red social de un tercero, se aproveche del cierto anonimato que le puede dar el uso de un pseudónimo.

Particularmente en Francia, tanto los servidores o espacios de alojamiento de información, como los editores de sitios web tienen la obligación legal de publicar su identidad en línea a efecto de encontrarse en aptitud de responder en caso de abuso o infracción.

La diferencia entre los espacios de alojamiento y los editores de información ha sido esclarecida por diversas jurisprudencias europeas y debates interminables desde el 2004, sin embargo, podríamos concluir que:

El editor de Internet es aquella persona que pone a disposición pública o carga contenido (texto, imágenes, audio, video, etc.) o que tienen la decisión editorial en sus manos sobre el contenido de otros, como sería el caso de los moderadores de foros, de grupos de Facebook, blogs, etc.

La decisión de la Corte de Justicia de la Unión Europea confirma que los editores de prensa en línea aún y cuando lo sean a título gratuito revisten el carácter de editores, con las responsabilidades que esto conlleva.

Por su parte, los espacios de alojamiento de información son aquellas personas físicas o morales que albergan contenido subido por otros sin haberlo filtrado o controlado previamente.

En este sentido, toda persona física o moral, es directamente responsable de aquello que publica en sus redes sociales, en calidad de editor, e incluso, en su calidad de espacio de alojamiento respecto de los contenidos que permite se suban en espacios sobre los que tiene un control directo, por ejemplo su muro de Facebook, tal sería el caso de una pregunta lanzada al público en una publicación (post) de Facebook que abriendo la puerta a un debate general, permite que otros usuarios de la misma red social carguen contenido, como texto, videos, archivos de movimiento o fotografías que pudieran ser de carácter ilícito.

La Ley mexicana por su parte, específicamente la Ley Federal de Protección al Consumidor, también obliga a los prestadores de bienes o servicios en Internet, a estar plenamente identificados y localizables, colocando a la vista en su propio sitio web, su nombre completo, domicilio físico y teléfonos de localización.

Para el caso de los sitios web que no son exclusivamente de carácter comercial, pero que se prevé tratamiento de datos personales, por ejemplo: un blog, un sitio web informativo o

académico, es aplicable la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que obliga a todo particular sea persona física o moral a contar con un aviso de privacidad, cuyo principal elemento es la identidad y domicilio del responsable del tratamiento de datos personales.

En este caso la responsabilidad del contenido recae directamente en la figura del responsable, valga la redundancia, y de manera indirecta en el encargado, es decir, en aquél externo a la organización del responsable que trata datos personales a nombre y por cuenta del responsable, como podría ser el servicio de alojamiento de información.

Aún y cuando las citadas leyes mexicanas no establecen en sí, una diferencia concreta entre el editor y el espacio de alojamiento, podríamos aplicar de forma supletoria la Ley Federal del Derecho de Autor.

Hablando de la Ley estadounidense, la regulación de los contenidos está marcada principalmente por la *Digital Millenium Copyright Act* y disposiciones de carácter civil, es decir, el establecimiento de políticas de *Notice and Take Down*, de contenidos a solicitud de las personas directamente afectadas, lo que el caso del desacato o desobediencia del proveedor de servicios de Internet, conlleva una responsabilidad solidaria y su consecuente sanción.

Si bien es cierto dado el criterio de competencia y jurisdicción, respecto del control de contenidos ilícitos en plataformas extranjeras, tanto la ley mexicana como la ley francesa, se encuentran ciertamente limitadas en la práctica.

Dependiendo del país, el proveedor de servicios de Internet se encuentra más o menos obligado a vigilar y sancionar los contenidos puestos a disposición pública a través de sus servicios y también varían las reglas aplicables en función del tipo de contenido, por ejemplo, la Ley estadounidense tiene una marcada orientación hacia la protección del copyright y la propiedad industrial y las legislaciones europeas más marcadas hacia el respeto a la vida privada y la protección de datos personales; la ley mexicana por su parte, presenta un híbrido sistema legislativo aplicable según el caso de que se trate.

Ahora bien, como podemos advertir, existen riesgos directamente ligados a nuestra información de carácter personal, mejor conocidos como datos personales, entendiendo que

varios de ellos conforman nuestra llamada identidad digital.

El interés por la protección de los datos personales, nace en diferentes momentos y en los tres países parte de nuestra investigación.

En el caso de Estados Unidos, cuya legislación es mucho más laxa y permisiva y no existe una Ley de carácter federal o general, sino normativa aislada y complementaria sectorial. Aún y cuando la primera referencia del derecho a la privacidad, data de 1890.

Los motivos que han dado origen a la protección de cierta información de manera sectorial obedecen a los fines para los cuales sea tratada la información y no contempla un estándar de protección en todas las áreas de la vida del ser humano, por ejemplo: respecto del comercio y la economía, la información de carácter personal reviste un nivel mínimo de protección, mientras que la información médica de una persona goza de un nivel más alto de protección.

El sistema de protección de datos personales vigente en Estados Unidos, en algunos casos es confuso y complejo, ya que los diferentes congresos estatales han establecido recomendaciones y parámetros de autorregulación muchas veces contradictorios entre si.

Vale la pena mencionar que gran parte de los esfuerzos que se han dado están motivados desde el exterior por los tratados de libre comercio y las relaciones comerciales con empresas de países cuya regulación en la materia es mucho más rígida, como es el caso de los países europeos.

Esa fue la causa de la implementación del *Safe Harbor Agreement*, empujado por la unión europea en mayo del año 2000.

La historia de Francia es diametralmente distinta, no sólo por las motivaciones de la Ley, por la fecha en la que comenzó a escribirse la historia de la protección de datos en este país, sino principalmente por el importante reconocimiento del derecho a la protección de datos personales como fundamental para la vida de los ciudadanos franceses.

Si bien es cierto que el concepto de *expediente* personal no es novedoso, sino que data de hace muchos siglos, específicamente con la entrada a nuestra vida de los dispositivos de tratamiento automatizado de información, también conocidos como sistemas informáticos, el manejo de

la información de forma masiva vio por primera vez la luz en la década de los 70's.

En el año de 1999 el Consejo Constitucional le otorgo al derecho a la vida privada el valor constitucional bajo el fundamento del artículo 2 de la Declaración de los Derechos del hombre y el ciudadano.

Mientras que el respeto a la vida privada fue incorporado al Código Civil francés en el año de 1970, en su artículo 9º que dispone que "cada persona cuenta con el derecho al respeto a su vida privada, Los jueces pueden, sin perjuicio de la reparación por daños y perjuicios, prescribir todas las medidas necesarias para hacer cesar una amenaza a la intimidad de la vida privada; estas medidas pueden en caso de urgencia ser ordenadas de forma cautelar.

Una referencia importante para nuestro estudio en complemento, fue el escrito del Tribunal de Gran Instancia de Paris del 13 de noviembre del año 2013 donde se profundiza el estudio del artículo 9º del Código Civil, precisando que toda persona tiene, en virtud del citado texto, el derecho exclusivo sobre su propia imagen, atributo de la personalidad, sobre la utilización de la misma; este derecho le permite, en principio, oponerse a la difusión de ésta sin su autorización y obtener la reparación de los perjuicios que este hecho le hubiera ocasionado.

Es importante precisar que el término "vida privada", es un concepto a geometría variable, que depende de diversos factores de hecho y de derecho, por ejemplo: una persona cuya actividad habitual pertenece a la vida pública, como es el caso de alguna actriz o cantante famosa, o bien, el caso de un funcionario público que por Ley debe transparentar algunas actividades de su vida, luego entonces, para la definición del concepto de "vida privada" para alguna resolución en específico, habrá que atender a las circunstancias del caso concreto, así como la situación precisa de la persona de la que se ha invadido este entorno de intimidad.

Sin embargo, más allá de la protección a la vida privada, encontramos un dominio de protección preciso que es el de la protección de los datos personales.

Es importante dividir el tema de la protección de datos personales de aquel de la vida privada, simplemente porque no todos los datos personales son de carácter privado y no todos los elementos que comprende nuestro entorno de intimidad refiere a datos personales.

Como lo hemos mencionado previamente, el nacimiento de los sistemas informáticos y las redes mundiales de comunicación, en particular, la Internet, vinieron a darle una nueva trascendencia y matiz a la protección de datos personales.

La Ley francesa que regula la protección de los datos personales es la Ley Informática y Libertades de 1978. En términos del artículo 2º de ésta, se entiende por dato personal "Toda información relativa a una persona física identificada o identificable ya sea de forma directa o indirecta". Como consecuencia de esta misma Ley, la creada en 1978 para la aplicación de la misma, fue la Comisión Nacional de Informática y Libertades (CNIL), como ente regulador de los datos personales de los ciudadanos franceses.

El derecho europeo de protección de datos personales, busca equilibrar por una parte la protección a la vida privada y la innovación y modernización de la economía mundial, respetando principios básicos de protección de datos personales, en particular el derecho francés, se funda sobre el derecho a decidir sobre el uso de los datos personales y controlar este uso, siguiendo los siguientes principios:

1. Información y consentimiento;
2. Los derechos de acceso, rectificación y oposición;
3. Finalidad del tratamiento;
4. Calidad;
5. Limitación del plazo de conservación; y
6. Seguridad.

Básicamente en los puntos citados anteriormente, son el fundamento y los principios rectores de la Ley mexicana.

La historia de la legislación mexicana en materia de protección de datos personales se escribió de forma distinta, vale la pena resaltar que de forma general, podríamos hablar de que desde los primeros visos de la misma, se planteó de manera aislada para los particulares y para el gobierno, independientemente de las iniciativas federales que tocaremos más adelante, los primeros avances que se dieron de forma específica, fueron de forma independiente, disposiciones apenas dibujadas para el gobierno en la Ley Federal de Transparencia y Acceso a la Información Pública

Gubernamental; y por otro dos de las propuestas locales aplicables a los particulares, mientras que la tercera propuesta de carácter local, le aplicaba a particulares y gobierno.

La primera Ley específicamente enfocada a la protección de datos personales en el país, no fue de carácter federal sino local, dicha iniciativa se presentó en el Congreso local en el año de 2000 en el Estado de Colima, aunque se promulgó hasta el 2003, en la exposición de motivos de la Ley, el legislador colimense, como en el caso de Francia, resalta la importancia de la protección de los datos personales en un entorno digital y no sólo eso, también atiende a la naturaleza de la información y los nuevos retos de la seguridad de la información cuando esta reside en medios informáticos y se comparte a través de redes de comunicación incluso fuera del país:

> *"…El avance tecnológico en materia de informática y de redes de cómputo en las últimas décadas ha sido extraordinariamente rápido y cada vez más incide en múltiples facetas de la actividad humana. En los últimos años, esto ha ido extendiéndose de manera importante hasta alcanzar a la población en general.*
>
> *De manera particular, el uso de información a través de sistemas digitales, ha permitido nuevas y más eficientes formas de prestar servicios a la población con elementos como el comercio electrónico, los servicios que ofrecen diferentes instancias del gobierno, sistemas de información y bases de datos, etc. Las ventajas que ofrece la tecnología de información son múltiples y muy importantes, por lo que cada vez es más utilizada.*
>
> *Evidentemente, es importante promover y facilitar el uso de las tecnologías de información. A nivel federal, existen lineamientos concretos para ello y en otros niveles de gobierno también se detectan intereses semejantes. En particular, en el Estado de Colima, la actual administración ha realizado importantes esfuerzos en este sentido.*
>
> *Sin embargo, es cada vez más clara la necesidad de que se brinde al ciudadano una protección adecuada contra el posible mal uso de la información que le concierne, sin que esto implique un*

intento de limitar o restringir los beneficios que pueden aportar las tecnologías de información.

Lo anterior deriva de que las nuevas tecnologías informativas ofrecen nuevas y más flexibles maneras de utilizar la información de manera inadecuada, poco ética y posiblemente perjudicial para el sujeto de la misma. Por ejemplo, los archivos tradicionales hacían muy difícil que pudiera cruzarse información de diferentes documentos, mientras que, estando digitalizada, esto resulta muy sencillo y rápido. Es claro que estas facilidades no son negativas, pero ofrecen a personas maliciosas, posibilidades nuevas, que conviene configurar como delictivas para protección de los individuos que pudieran ser afectados. La legislación vigente no contempla muchas de estas acciones como delictivas, ya que antes no resultaban factibles en general.

Muchos países ya han detectado estas nuevas condiciones y se han iniciado una gran cantidad de esfuerzo para tomar las medidas pertinentes y acordes a las diferentes condiciones locales. De particular interés es la directriz generada por la Comunidad Europea, aunque existen otros muchos ejemplos de posible interés para inspirar una posible legislación en Colima.

En México, el marco jurídico para estos aspectos aún no se desarrolla de manera adecuada. Recientemente se realizaron modificaciones al Código Penal en el ámbito federal, orientadas a proteger la información en los equipos de cómputo, y en diferentes ordenamientos para facilitar el desarrollo del comercio electrónico. Sin embargo, la protección al ciudadano es incompleta.

Se ha ido detectando una preferencia por legislar de manera genérica, tratando de configurar las conductas delictivas dentro de una visión general, evitando caer en legislaciones de carácter específico para los aspectos electrónicos o digitales. Conviene aplicar este criterio en materia de protección a la privacía, ya que, de otro modo, se

podría caer en el riesgo de que ciertas acciones fueran legales en un ambiente digital, e ilegales cuando se realizan con medios convencionales, o viceversa.

El problema de la privacía tiene elementos complejos, derivados de la propia naturaleza y características de la información y de los diferentes ámbitos de su utilización…"

La Ley de Protección de Datos del Estado de Colima del 14 de junio de 2003, se funda en la Constitución Política del Estado Libre y Soberano de Colima, en su artículo 1º, reconociendo plenamente al Derecho de Protección de Datos de Carácter Personal como un Derecho Humano fundamental.

Dicha Ley encuentra amplia inspiración en la legislación europea y en algunos puntos tiene marcadas diferencias con la Ley Federal de 2010, por ejemplo, el concepto de Dato Personal.

"Datos de carácter personal: los datos relativos a personas físicas o morales que de manera directa o indirecta puedan conectarse con una persona específica. Se incluyen a manera ilustrativa, datos representados en forma de texto, imágenes, datos biométricos como la huella digital, datos sobre el DNA de las personas o cualquier otro que corresponda intrínsecamente a una persona determinada."

Respecto de este concepto, no estamos de acuerdo con incorporar los datos de las personas morales, ya que por una parte una persona moral es una ficción jurídica y por la otra, es información de interés público, tan es así que vive en registros públicos para consulta de los interesados.

En el caso del Estado de Jalisco, segundo en orden de aparición, el legislador jalisciense decidió que no era necesario crear una Ley específica que regulara el tema de la protección de los datos personales, sino que consideró que era mejor incorporar una disposición al respecto en el Código Civil para el Estado de Jalisco, por tal motivo, el 18 de septiembre de 2004, se adicionó un Capítulo completo, el III, denominado "De la información privada", al Título "De las personas físicas", añadiendo el artículo 40 y 40 BIS, que a la letra citaba:

"…Mediante esta iniciativa me propongo regular la información privada. La cada vez más compleja competencia económica ha propiciado que la legislación privilegie los fenómenos del mercado, olvidándose cada día más de la humanización de las relaciones sociales. Los vínculos entre el mercado y los consumidores son cada vez más violentos, llegándose incluso a un libertinaje en el campo de la urbanidad, cuando de ganar espacios en el mercado se trata. En esta vertiginosa lucha por la conquista de un mayor número de consumidores, las estrategias de la mercadotecnia no han vacilado en invadir la vida privada de la gente y las corporaciones. Hoy como nunca antes, los datos personales circulan por el mundo del comercio sin orden ni control. El ciudadano ordinario no sabe quienes [sic] tienen acceso a sus datos personales, ya no se diga nombre, sexo, edad y estado civil, sino domicilio, empleo, ingresos, familia y hasta religión y raza.

[...]La información privada no debe circular sin el consentimiento de su titular. No es políticamente viable que esta información sea transmitida de archivo en archivo, sin que el titular tenga ingerencia [sic] en ese tráfico.

[...] El arribo de la informática a la vida social ha sembrado un verdadero caos en el uso y transferencia de información privada. Creo que no es legítimo que se manipulen nuestros datos sin nuestro consentimiento, y por el contrario, estimo conveniente que se responda por los daños materiales y morales que pudieran producirse por el uso indebido y desautorizado de la información privada.

[...] Se considera de importancia creciente que la gente cuente con instrumentos legales que pongan freno al uso indiscriminado de su información privada…"

El entonces capitulado quedó de la siguiente manera:

"CAPTULO III
De la información privada

Artículo 40 Bis 1.- Información privada es la que se

genera a partir de los datos referidos a una persona física, cuya divulgación no esté prevista en disposiciones de orden público.

Artículo 40 Bis 2.- Los datos de las personas físicas constituyen un derecho que sólo corresponde disponer al titular en los términos de la ley.

Artículo 40 Bis 3.- Son datos personales las referencias personales de cualquier tipo, tales como nombre, domicilio, estado civil, empleo, escolaridad o cualquier otra que describa la situación o estado de la persona con relación a su vida familiar, social o laboral.

Se consideran datos sensibles la información personal que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación política e información referente a la salud o a la vida sexual.

Son datos informatizados, los personales sometidos al tratamiento o procesamiento electrónico o automatizado.

Artículo 40 Bis 4.- Es titular de los datos toda persona física con domicilio en el Estado de Jalisco, cuya información sea objeto del tratamiento al que se refiere este capítulo.

Artículo 40 Bis 5.- La administración de información privada que posean instituciones públicas se regirá por la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco, las demás leyes de la materia y este capítulo, en su caso

.

Artículo 40 Bis 6.- Los datos personales sólo pueden ser utilizados para fines lícitos.

Artículo 40 Bis 7.- Los registros de datos personales deben contener información cierta, adecuada, pertinente y no

excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

Artículo 40 Bis 8.- La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de este capítulo.

Artículo 40 Bis 9.- Los datos personales no pueden ser utilizados para finalidades distintas a las que motivaron su obtención.

Artículo 40 Bis 10.- Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados por el responsable del archivo o base de datos, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecido en este artículo.

Artículo 40 Bis 11.- Sea cual fuera la forma de almacenamiento de datos o la persona que posea la información, el titular tiene derecho de acceso a los mismos para imponerse de su contenido.

Artículo 40 Bis 12.- Quien administre registros de datos personales deberá distribuirlos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

De la destrucción se deberá levantar acta circunstanciada ante notario público o dos testigos.

Artículo 40 Bis 13.- La información personal contenida en registros particulares puede transferirse a terceros mediante convenio suscrito con arreglo a este capítulo.

Artículo 40 Bis 14.- El uso de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado.

Artículo 40 Bis 15.- No será necesario el consentimiento cuando:

I. Los datos se obtengan de fuentes de acceso público irrestricto;

II. Se recaben en virtud de una obligación legal;

III. Se trate de listados cuyos datos se limiten a información que obre en registros públicos;

IV. Deriven de una relación contractual del titular de los datos, y resulte necesario su uso para el desarrollo o cumplimiento de una obligación;

V. Se trate de datos que tengan fines estadísticos y se despersonalicen de tal forma que no puedan ser vinculados con el titular; y

VI. Se trate de información recabada sin fines de lucro, destinada a apoyar instituciones de beneficencia pública.

Artículo 40 Bis 16.- Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

I. La finalidad del registro y quiénes pueden ser sus destinatarios o clase de destinatarios;

II. La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable;

III. El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga;

IV. Las consecuencias de proporcionar los datos, de la negativa de hacerlo o de la inexactitud de los mismos; y

V. La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Artículo 40 Bis 17.- Queda prohibida la formación y transferencia de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles de la persona.

Artículo 40 Bis 18.- Los datos sensibles sólo pueden ser recolectados y objeto de registro y transferencia cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

Artículo 40 Bis 19.- Los establecimientos y profesionales vinculados a los servicios de salud pueden recolectar y tratar los datos personales relativos al estado físico o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, debiendo guardar en secreto los datos del paciente.

Artículo 40 Bis 20.- El responsable o usuario del archivo de datos debe adoptar medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permita detectar desviaciones de información.

Artículo 40 Bis 21.- El responsable y las personas que intervengan en cualquier fase de registro o transferencia de datos personales están obligados al secreto profesional respecto de

los mismos. Tal obligación subsistirá aún después de finalizada su relación con el titular del archivo de datos.

Artículo 40 Bis 22.- Los datos personales objeto de registro sólo pueden ser transferidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente.

Artículo 40 Bis 23.- El consentimiento para la transferencia de información personal será revocable hasta que no se lleve a cabo la operación.

Artículo 40 Bis 24.- Toda persona en cuanto titular de los datos, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos privados destinados a proveer informes.

Artículo 40 Bis 25.- El poseedor de información personal tiene la obligación de proporcionar la información que se le solicite en los términos de la fracción anterior dentro de los diez días siguientes a la presentación de la solicitud.

Artículo 40 Bis 26.- El derecho de acceso a la información personal en registros privados por parte del titular será ejercido en forma gratuita.

Artículo 40 Bis 27.- El ejercicio del derecho a que se refiere la fracción anterior, respecto a los datos de personas fallecidas le corresponderá a sus sucesores.

Artículo 40 Bis 28.- En ningún caso el informe que rinda el registro podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

Artículo 40 Bis 29.- El responsable o usuario de un registro o banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de haber recibido la solicitud del titular de los datos o advertido el error o falsedad.

No procede la supresión de los datos cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

Artículo 40 Bis 30.- Los datos personales deben ser conservados durante los plazos previstos en las disposiciones contractuales que se hubieren suscrito entre el responsable o usuario del banco de datos y el titular de los datos.

Artículo 40 Bis 31.- Los responsables de bancos de datos privados denegarán el acceso, rectificación o la supresión de datos de carácter personal en función de la protección de los derechos e intereses de terceros.

Artículo 40 Bis 32.- La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros privados se efectuará sin cargo alguno para el interesado.

Artículo 40 Bis 33.- Las personas que transfieran archivos, registros o bancos de datos con finalidad de lucro, deberán tener dentro de su objeto social dicha actividad.

Artículo 40 Bis 34.- En la prestación de servicios de

información para el otorgamiento de créditos sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

Artículo 40 Bis 35.- Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho. En los casos de datos originados en concursos este plazo se extenderá a diez años.

Artículo 40 Bis 36.- La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos, cuando su sesión esté relacionada con el giro de las actividades comerciales o crediticias de los cesionarios.

Artículo 40 Bis 37.- Se podrán recabar datos personales cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. Solo se podrá ceder a un tercero esta información en forma total o parcial si cuenta con el consentimiento expreso y previo del titular de los datos, pudiendo esta conformidad para cesiones posteriores ser prestada en el momento de la recopilación.

Artículo 40 Bis 38.- Las disposiciones de este capítulo no se aplicarán a las encuestas de opinión, mediciones, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

Artículo 40 Bis 39.- Quien administre información privada y afecte su titular responderá por los daños y perjuicios derivados

de la inobservancia de este capítulo."

Consideramos prudente mencionar el articulado adicionado, ya que como podemos advertir, si bien, es cierto que es de reconocer la iniciativa del legislador jalisciense de incorporar normativa innovadora en ese tiempo al Estado de Jalisco, la redacción no fue tan afortunada, además de que a lo largo de lo que terminaron siendo en realidad 40 artículos, no termina por darle al titular de los datos personales la tan anhelada seguridad jurídica respecto de la correcta tutela de su información.

Este esfuerzo no cristalizado, tuvo su fin en el año de 2009, con la publicación del Decreto de Reforma Constitucional que mencionaremos más adelante.

La historia de la legislación del Estado de Tlaxcala, obedece a una historia peculiar, se trata de la creación de una Ley de Transparencia y Acceso a la Información Pública, a la que se incorpora el tema de protección de datos personales, en el año de 2007, quedando de la siguiente manera:

Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Tlaxcala.

Se reconoce también, el esfuerzo del legislador tlaxcalteca al buscar la incorporación de un tema tan importante y hasta ese año de 2007, tan poco aterrizado a la legislación mexicana, sin embargo, creemos que presentaba importantes áreas de oportunidad y sin duda, a pesar de ser un precedente a destacar, no era suficientemente bueno.

A lo largo de las definiciones, varias de ellas eran oscuras y ambiguas, por ejemplo:

"…Artículo 2.-…

…Son datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Artículo 3. En materia de datos personales no se podrán afectar los registros y fuentes periodísticas, y es aplicable a los datos de carácter personal que obren

en archivos, registros, bancos o bases de datos de las personas físicas o morales, así como de las entidades públicas.

Todo uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado deberá observar lo dispuesto en esta ley.

Artículo 4.-…

… V. Datos personales: La información que unívocamente distingue a un individuo de otro. Incluye no sólo a las llamadas "calidades generales", sino también el origen étnico o racional, la filiación religiosa o ideológica, las preferencias sexuales, etc…

… XII. Registro de datos: Conjunto de datos personales, organizados y tratados automatizadamente en archivos, registros, bases o banco de datos;

XIII. Tratamiento de datos: Operaciones y procedimientos sistemáticos que tienen por objeto obtener, guardar, ordenar, modificar, relacionar, cancelar y cualquiera otra que implique el procesamiento de datos, o su cesión a terceros a través de comunicaciones, consultas, interconexiones y transferencias;

XIV. Responsable de los datos: Persona física o jurídica que ostenta la titularidad del archivo, registro, banco o base de datos;

XV. Datos informáticos: Los datos personales tratados automatizadamente;

XVI. Usuario de datos: Toda persona física, jurídica o entidad pública que trata datos personales de manera voluntaria, ya sea en archivos, registros, bancos de datos propios o a través de conexión con los mismos;

XVII. Disociación de datos: Todo tratamiento de datos personales que impida asociarlos a persona identificada o identificable, y

XVIII. Interesado: La persona física titular de los datos personales.

XIX. Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno.

XX. Datos: Un dato es la unidad o cantidad mínima de información no elaborada, sin sentido en sí misma pero que convenientemente tratada se puede utilizar en la realización de cálculos o toma de decisiones."

En el entendido de que la citada Ley ha sido posteriormente reformada, y sólo nos sirve como referencia de uno de los tres primeros instrumentos legislativos en materia de protección de datos personales en nuestro país, haremos sólo unas breves reflexiones al respecto:

1. La definición de datos sensibles es ciertamente ambigua y no atiende al espíritu del legislador europeo al momento de clasificar cierta información como datos sensibles, nos parece ciertamente temerario el hecho de que se hable de los hábitos de una persona como dato sensible sin que se entienda que esta información no forzosamente debería ser clasificada como tal si es que no le implica ningún riesgo grave para su moral o patrimonio, por ejemplo: si una persona todos los días tira la basura a las 7 de la mañana, eso no debería ser considerado como dato personal, cosa distinta es que se revele que todos los días 17 de cada mes, a las 7 de la mañana tira a la basura todos sus estados de cuenta bancarios porque es una fecha después del corte y no le gusta almacenar esos papeles en su casa, luego entonces la sensibilidad sigue recayendo en la información contenida en el documento identificado como estado de cuenta bancario, mas no específicamente sobre el hábito de la persona, ya que este riesgo puede disminuir por el sólo hecho de que esos estados de cuenta lleguen a la basura previa y debidamente triturados, de forma tal, que sean inaccesibles a personas malintencionadas.

2. Al hacer referencia expresa a los datos que obren en fuentes periodísticas deja fuera por completo la posibilidad del llamado "Derecho al Olvido", al menos no en lo que toca a datos personales, es decir, que un diario de circulación estatal, estaría obligado, en ejercicio del derecho de réplica a hacer aclaraciones respecto de lo imputado injustamente a una persona, mas no a borrar su nombre, por lo que, a nuestro punto de vista seguiría dejando en el espíritu del lector, una duda razonable, podremos un ejemplo al respecto:

Nota periodística: “Juan Pérez es arrestado por homicidio y será condenado a pagar una condena de hasta 50 años de prisión”

Realidad: Juan Pérez asistía a su vecina de una casa de huéspedes, una anciana que murió de forma natural durante la madrugada de un jueves y el día viernes, Juan acudió a su morada como cada mañana a saludarla y al percatarse de que no respiraba más, la toma en sus brazos para tratar de hacer alguna maniobra de resucitación, la dueña de la casa de huéspedes entra a la habitación de la anciana e inmediatamente llama a la policía, quien al encontrar a la mujer sin vida, se lleva a Juan a la Delegación para que presente su declaración, un medio local capta la historia a su manera, aduciendo inmediatamente la comisión del delito de homicidio por parte de Juan.

En términos de la Ley, tal y como se encontraba redactada, Juan no habría tenido derecho a que se eliminara su nombre por completo de la nota periodística, sino únicamente a que el reportero hiciera una aclaración de su grave falta de profesionalismo y ética, y quedaría para siempre la referencia en un número anterior, de que Juan fue un homicida, lo que podría afectarle incluso en su ámbito laboral.

4. Esta Ley se contradice continuamente ya que no es clara respecto de si es menester o no que el tratamiento de datos se dé de forma automatizada o sistematizada, razón por la cual, en la práctica, hubiera dejado fuera mucha información de carácter personal contenida en archivos en papel y no debidamente administrados.

5. La definición que aporta la Ley, de lo que es un dato personal, también deja fuera muchas posibilidades, ya que un domicilio de una casa de huéspedes no sería un dato personal, ya que no identifica unívocamente a una persona sino a todos sus habitantes, y después en la misma redacción, incluye cierta información clasificada internacionalmente como dato sensible como la religión o las preferencias sexuales.

6. Las definiciones de “Dato informático”, “Registro de Datos”, “Tratamiento” y “Disociación”, también nos parecen muy poco afortunadas.

7. Respecto del término “interesado”, la Ley lo confunde con el titular, ya que interesado es un concepto procesal que podría revestir cualquier persona que compruebe un interés jurídico,

por ejemplo, si el titular de los datos es un menor de edad, el interesado sería su padre o tutor.

Por último, en el concepto "Usuario de los datos", cabe aclarar que las entidades públicas están sujetas no al actuar de su voluntad sino aquél que por mandato de Ley les ha sido específicamente permitido, así que no le sería aplicable esta definición.

Habiendo agotado ya el pasaje breve de los antecedentes legislativos en México, es importante destacar que con anterioridad a estas disposiciones legislativas ex profeso, nuestro país ya contaba con regulación sectorial, un esquema muy parecido al estadounidense.

Las leyes aplicables a diferentes sectores económicos del país contienen disposiciones relativas a la protección de los datos personales, por ejemplo: el secreto bancario en la Ley de Instituciones de Crédito, el secreto profesional mencionado en la Ley General de Salud.

A continuación, presentamos una tabla con las disposiciones en materia de protección de datos personales por sector o rama de la industria.

En materia de Transparencia, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental del año 2002, menciona en su capítulo

Como ya hemos mencionado anteriormente, la evolución legislativa de cada país obedece a diversas circunstancias meta jurídicas, es decir, socio políticas y económicas que llevan a generar este proceso por motivaciones incluso de índole supra nacional.

La primera iniciativa de Ley Federal data del año 2000, a lo largo de casi diez años, se presentaron diversas iniciativas con distintos matices, unas más apegadas a la directiva europea y otras más al modelo norteamericano (Estados Unidos y Canadá).

En el año de 2009, después de largas negociaciones, se modifica la Constitución Política de los Estados Unidos Mexicanos, en sus artículos 6º, 16 y de 73 para dar paso a la que sería la primera Ley Federal en la materia.

El Artículo 6º, garante del derecho a la libertad de expresión y del acceso a la

información, se modificó el 20 de julio de 2007 para darle facultades al entonces Instituto Federal de Acceso a la Información Pública Gubernamental, para poder ser competente en el ámbito de la protección de datos personales:

"Artículo 6.- ...

VIII. La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.

El organismo autónomo previsto en esta fracción, se regirá por la ley en materia de transparencia y acceso a la información pública y protección de datos personales en posesión de sujetos obligados, en los términos que establezca la ley general que emita el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho.

En su funcionamiento se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

El organismo garante tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal; con excepción de aquellos asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación, en cuyo caso resolverá un comité integrado por tres ministros. También conocerá de los recursos que interpongan los particulares respecto de las resoluciones de los organismos autónomos

especializados de las entidades federativas que determinen la reserva, confidencialidad, inexistencia o negativa de la información, en los términos que establezca la ley."

Al Artículo 16, históricamente conocido por garantizar la legalidad de las actuaciones de la autoridad, así como la no molestia por parte de ésta en el ámbito privado, es decir, el Derecho a la vida privada; se le añade un segundo párrafo en el cual, por primera vez en la historia de nuestro país, se reconoce el Derecho Humano y ahora Constitucional a la protección de los datos personales de los mexicanos.

Luego de la reforma, el segundo párrafo del artículo 16, quedó de la siguiente manera:

"Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."

El Artículo 73, fue estratégicamente reformado para dotar de facultades al Congreso de la Unión, y adicionar la fracción

"XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares"

Mencionamos "estratégicamente", porque lo que en ese momento buscaba el legislador federal, era evitar la creación de leyes "locales" que fueran más laxas y a su vez evitar la

generación de paraísos libres de protección de datos o con obligaciones mínimas al respecto.

Es así como en el año 2009 terminan de sentarse las bases de lo que sería la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

De manera extraoficial, podemos decir, basados en la intuición, que el aspecto económico tuvo sin duda un papel muy importante y decisivo en el nacimiento de esta Ley, ya que, justo como lo indicamos previamente, fueron casi diez años de negociaciones e iniciativas de casi todos los grupos parlamentarios sin que pudiera llegarse a un acuerdo, gobierno, sociedad civil e industria, hasta el año de 2010.

Es importante destacar, que en gran medida la connotación económica de esta Ley, se marcó en función del valor económico del dato per se, por el uso y explotación del mismo en las diversas ramas de la industria mexicana.

CAPÍTULO II: LA EVOLUCIÓN DE LA COOPERACIÓN INTERNACIONAL EN LA LUCHA CONTRA LAS VIOLACIONES A LA IDENTIDAD DIGITAL.

La naturaleza misma del cibercrimen, hacen que este no conozca de fronteras ni de jurisdicciones, ataques que se orquestan en China o Europa del Este, pueden estar dirigidos hacia Estados Unidos o Israel.

Tan importante es contar con legislación nacional para hacer frente a las infracciones de carácter penal cometidas por medios informáticos, como el contar con eficaces convenios de cooperación internacional y, sobre todo, con organizaciones internacionales que permitan seguir el rastro de la delincuencia organizada.

Actualmente existen diversos organismos internacionales llevando a cabo esfuerzos contra la cibercriminalidad, por ejemplo:

- La Organización de Estados Americanos (OAS por sus siglas en inglés)
- El Consejo de Europa

- La Unión Internacional de Telecomunicaciones
- El Foro de Cooperación Asia Pacífico
- INTERPOL
- EUROPOL

Las citadas instituciones han sido fundamentales para el combate a diversos tipos de crímenes, la investigación y sobre todo la cooperación internacional para la investigación de éstos.

Una de las propuestas de este trabajo es precisamente hacer uso de los instrumentos de cooperación internacional vigente en aras de que el combate al cibercrimen se sume a las tareas que se llevan a cabo en el marco de estos acuerdos de cooperación.

Por ejemplo, INTERPOL cuenta con 192 países miembros, por lo que se erige como la mayor organización policial del mundo, dentro de sus actividades, se encuentran la capacitación policial y la cooperación en la investigación de delitos y captura de delincuentes.

En el último año se ha incorporado a sus herramientas de trabajo, una base de datos internacional de identidades conocido como I-Checkit, la cual permite controlar la información de individuos que cruzan las fronteras de los países a través de los medios de transporte pero que también permite cruzar información con las entidades bancarias, lo cual ayudaría increíblemente a rastrear los recursos obtenidos de forma ilícita.

En resumen, la propuesta es clara, a pesar de que aún faltan acuerdos multilaterales e internacionales por firmar, que fomenten la cooperación en materia de cibercrimen, hacemos énfasis en que las herramientas vigentes pueden ser excelentes alternativas para perseguir a los ciberdelincuentes y frenar los recursos con los que operan.

CAPÍTULO III: LA CONTRIBUCIÓN DE LA INICIATIVA PRIVADA Y LA AUTORREGULACIÓN COMO ALTERNATIVA PARA EL COMBATE A LAS VIOLACIONES A LA IDENTIDAD DIGITAL.

El tema de la autorregulación ha sido especialmente polémico en los últimos años, la autorregulación nace desde el ser humano como una forma de regular emociones, acciones comportamientos y se extiende hacia las organizaciones, y se define como aquella capacidad de la que dispone una entidad, asociación, organización o institución de regularse a sí misma con base en un monitoreo y control voluntario.

Es precisamente esto último, lo que genera una interesante polémica, ya que al dejar la libertad de autoevaluarse y posteriormente implementar las mejores y correcciones pertinentes a las propias organizaciones, es prácticamente dejar una puerta abierta al incumplimiento.

A pesar de que es una alternativa viable y comprobada por los gobiernos estadounidenses, canadienses y recientemente reconocida por la autoridad francesa y el Reglamento General de Protección de Datos del Parlamento Europeo y del Consejo Europeo; existe bastante escepticismo en los gobiernos y en la población.

En lo que respecta a México, desde hace más de una década, el gremio de las empresas proveedoras de servicios de Internet se han enfocado en trabajar en la creación de un Sello de Confianza, que permite a las empresas que se afilian a este programa el adherirse a un mecanismo de evaluación gremial en pro de los consumidores.

Al final de los años 90’s, a iniciativa del Canadian Institute of Chartered Accountants (CICA) y del American Institute of Chartered Public Accountants (AICPA)” nacen los “sellos de confianza”, y fueron el detonante para que otras empresas del sector privado empresarial apoyaran este tipo de prácticas en diversas partes del mundo.

Los Sellos de Confianza son marcas (distintivos) principalmente electrónicas, otorgadas por alguna entidad privada, que se publican en las páginas Web e indican que el proveedor cumple con las leyes, códigos éticos y de buenas prácticas; brinda una mayor seguridad tecnológica y procedimental antes, durante y después de la transacción; además, establecen mecanismos alternativos para resolver controversias entre comprador y vendedor.

La autorregulación constituye una herramienta útil para los sectores comerciales o de servicios, porque se ajusta a necesidades cambiantes y, por tanto, hace flexible su modificación, sin tener que pasar por el complejo aparato legislativo.

La autorregulación ha surgido como la reglamentación derivada de la autonomía privada de empresarios que tratan datos, o de las organizaciones en que se agrupan para adoptar códigos deontológicos de conducta. La autorregulación se ha fomentado desde la OCDE y también es una posibilidad contemplada en la Unión Europea en diversas disposiciones sobre tratamiento de datos personales, protección de la intimidad en las comunicaciones electrónicas y sobre el comercio electrónico. De igual forma, el grupo de Cooperación Económica Asia-Pacífico (APEC), en su proyecto Data Privacy Pathfinder, tiene el propósito de analizar e identificar las mejores prácticas en materia de privacidad y el rol de los sellos de confianza como impulsores del flujo de información a nivel internacional.

La iniciativa Pathfinder promueve el trabajo conjunto entre sector privado, gobiernos, organizaciones de consumidores y grupos de interés público en aspectos de privacidad y protección de datos, para desarrollar un sistema que permita al sector privado crear reglas globales para la protección de la privacidad de los datos personales, apoyándose en el uso de sellos de confianza para el consumidor (trustmarks).

El objetivo es encontrar un balance entre liberar el intercambio de información electrónica para propiciar el desarrollo del comercio electrónico; al tiempo que da certeza a los ciudadanos, garantizándoles la protección y el buen uso de datos de carácter privado.

En México fue hasta el año 2007 cuando surgen los sellos de confianza, promovidos por algunas empresas representantes de la industria como una forma de hacer ver a los legisladores que también a la industria le interesaba contar con una legislación adecuada en materia de protección de datos personales.

Desde su concepción, se sometieron al Marco sobre privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC por sus siglas en Ingles) a través de avisos de privacidad y sus respectivos resúmenes.

El proyecto fue impulsado por la Asociación Mexicana de Internet (AMIPCI), con

el apoyo del Gobierno Federal a través de la Secretaria de Economía (Fondo PROSOFT).

La AMIPCI revisa que la empresa o Institución que cuenta con un sitio Web en operación y que solicita el sello, cumpla con cuatro aspectos:

1. Cumplir con el marco legal aplicable a cada sector:

   a) El sector privado debe ajustarse a lo señalado por la Ley Federal de Protección al Consumidor respecto de proporcionar en el Sitio Web números telefónicos, dirección y demás información de la organización, que permitan al comprador realizar aclaraciones o reclamaciones; usar la información recabada sólo para los fines solicitados garantizando la confidencialidad de la misma y no ceder dicha información a terceros; evitar prácticas de envío de mensajes no solicitados, y eliminar las prácticas comerciales engañosas.

   b) El sector público debe cumplir con lo señalado en Ley Federal de Transparencia y acceso a la información Pública y los Lineamientos de Protección de Datos Personales.

2. Sujeción al Marco sobre privacidad de la APEC, a través de avisos de privacidad y sus respectivos resúmenes.

3. Observancia del Código de Ética de la AMIPCI.

4. Cumplimiento de los términos y condiciones establecidos en el contrato celebrado entre la AMIPCI y los titulares del sello.

Al cumplir con estos cuatro puntos se otorga el sello de confianza, y con ello se reconoce a las empresas o instituciones que promueven el cumplimiento de la privacidad de la información y están legítimamente establecidas. AMIPCI también ofrece como mediación un procedimiento entre las partes para resolver controversias entre los consumidores y los titulares del sello.

Actualmente existen cerca de 400 sitios Web que ya cuentan con este distintivo único en su tipo en nuestro país.

En el ámbito internacional, desde noviembre de 2007, la AMIPCI suscribió el Memorándum de Entendimiento con TradeSafe y ECNetwork de Japón, SOSA de Taiwán; el Instituto de Comercio Electrónico de Corea del Sur; CommerceNet y Case Trust de Singapur y TRUSTe de los Estados Unidos, que son los principales proveedores de servicios de sellos de confianza de la región Asia Pacífico y que conforman la Asia-Pacific Trustmark Alliance (ATA). En virtud de dicho Memorándum, la AMIPCI se integra formalmente a la ATA, mediante el Sello de Confianza AMIPCI, y participa en el "Pathfinder de Privacidad de APEC" y es compatible con los sellos de confianza de dicha organización regional.

Con la incorporación al grupo del sello de confianza Euro-Label se constituyó la World Trustmark Alliance.

Destaca también la suscripción, el 20 de noviembre de 2008, en el marco del "II Congreso E-Commerce Latam 2008", del Memorándum de Entendimiento entre la AMIPCI y la Cámara de Comercio Electrónico de Colombia, la Asociación Española de Comercio Electrónico y Marketing Relacional, la Cámara de Comercio de Santiago de Chile, la Cámara Brasileña de Comercio Electrónico y la Cámara Argentina de Comercio Electrónico. Las organizaciones firmantes se comprometieron a trabajar conjuntamente para la definición de un marco normativo para facilitar la adopción, el uso y el reconocimiento recíproco de sellos de confianza a nivel de Iberoamérica.

En el breve tiempo de su existencia, el Sello de Confianza de la AMIPCI se ha convertido en un método de autorregulación ampliamente reconocido en México para la certificación de las políticas de privacidad y existencia física, que, a la luz de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, deberá evolucionar como un mecanismo legalmente válido para que la industria alcance estándares mundiales en sus prácticas de comercio electrónico confiable.

Otro de los mecanismos reconocidos por la Ley mexicana, particularmente la legislación en materia de protección de datos personales es un esquema de autorregulación vinculante, es decir, una actividad a través de la cual el responsable, como aquella persona que decide sobre el tratamiento de datos personales, o el encargado, quien individual o conjuntamente con otras trate datos personales por cuenta del responsable, se comprometen de manera voluntaria a la protección de éstos.

Los esquemas de autorregulación vinculante están basados en los parámetros emitidos por la Secretaría de Economía, en coadyuvancia con el INAI, y permiten armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares de los mismos, así como la prevención de consecuencias y medidas correctivas eficaces en caso de incumplimiento a tales esquemas.

Estos esquemas de autorregulación vinculante están constituidos por dos elementos básicos: por un lado, el tipo de esquema de autorregulación vinculante en el que se recogen los principios, normas y procedimientos que los miembros adheridos se comprometen a observar y cumplir y, por otro lado, los mecanismos de control necesarios para su aplicación.

CAPÍTULO IV: EL DESARROLLO DE HERRAMIENTAS DIGITALES EN LA LUCHA CONTRA LOS ATAQUES A LA IDENTIDAD DIGITAL.

« Le moyen d'être sauf, c'est de ne pas se croire en sécurité »
Thomas Fuller

Lo que solemos llamar seguridad, no es otra cosa que una forma de sentir y que su mayor aproximación es la minimización del riesgo, éste último, estado natural de la vida; el diccionario de la Real Academia Española, define la seguridad como una cualidad, la cualidad de seguro, y a su vez, conceptualiza a lo seguro como algo libre y exento de riesgo, algo que brinda certeza y confianza; es así, que la seguridad depende directamente del riesgo, no existen el uno sin el otro y suelen ser inversamente proporcionales, es decir, a menor riesgo mayor seguridad y viceversa.

No hay manera de concebir una medida de seguridad sin una correcta dimensión del riesgo. Por tanto, es un concepto a geometría variable.

El tema de la seguridad de la información cobra relevancia, cuando dimensionamos la importancia de salvaguardar la confidencialidad[127] de la misma; en el ámbito de la protección de datos personales, la confidencialidad y la seguridad son dos conceptos íntimamente relacionados cuyo fin es garantizar que no se haga un uso indebido de la información con carácter de dato personal. Sin embargo, aún dentro de la categoría de datos personales, alguna de esta información, requerirá de medidas de seguridad más altas que el resto.

Por ejemplo, ya que un dato personal[128] es toda aquella información concerniente a una persona física identificada o identificable, podemos inferir que dentro del vasto universo que plantea el concepto contenido en nuestra Ley mexicana (Ley Federal de Protección de Datos Personales en Posesión de los Particulares), existe una gran cantidad de información que podría clasificarse como tal, pero no toda ella merece el mismo nivel de confidencialidad, por lo que el dato que corresponde a mi nombre completo no tendría el mismo peso específico que mi historial crediticio o más aún mi historial médico.

[127] El término confidencialidad que proviene confidencia y a su vez de la palabra confianza, es además uno de los dos deberes contemplados en el artículo 9º reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; en relación con los artículos 19 y 21 de la Ley.
[128] Artículo 3 fracción IX, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En este nuevo paradigma de la sociedad de la información[129] y la dependencia de las herramientas informáticas[130], es casi un sinónimo de muerte civil no aparecer en los buscadores ¡Quién eres si no apareces en Google!, si la Internet no "constata" o "relata" tu historia; puede ser muy atractivo para mí ser una persona cuyos resultados de búsqueda se extiendan a diversas páginas, o puede no serlo, eso dependerá de mi nivel de exposición, y de nuevo, el riesgo que esta conlleve, sin embargo, cualquiera que sea el caso, no debe ser un asunto ligero el que se exhiba el historial médico de un individuo y mucho menos sin su consentimiento, la mayoría de las personas podrían sentirse incómodas ante tal situación.

Cada vez se vuelve más difícil guardar el equilibrio entre lo público y lo privado, entre la exposición y la discreción, sobre todo cuando la seducción de la aparente fama nos impide visualizar potenciales riesgos, eso lo saben muy bien los cientos de personas que han sido "linchadas virtualmente" gracias a un irresponsable uso de las tecnologías de la información y la comunicación.

Las medidas de seguridad que, por Ley[131], deben acatar los responsables que traten datos personales, no pueden de ninguna manera definirse sin antes conocer a detalle el nivel de riesgo, y por ello se entiende un análisis holístico de este concepto.

Delimitar el nivel de riesgo conlleva la puesta en marcha de toda una metodología de análisis[132], que comienza con la identificación de los datos personales que se tratan, el propio alcance del tratamiento, pasando por los medios de almacenamiento y llegando hasta la capa más vulnerable que es la humana, es decir, todas aquellas personas que por motivo de su empleo o de su encargo, tendrán acceso a esa información.

---

[129] Sociedad de la información, es un término que fue introducido desde 1973 por el sociólogo Daniel Bell, quien *formula que el eje principal de ésta será el conocimiento teórico y advierte que los servicios basados en el conocimiento habrían de convertirse en la estructura central de la nueva economía y de una sociedad apuntalada en la información, donde las ideologías resultarían sobrando.* Bell, Daniel, *The coming of Post-Industrial Society A venture in social forecasting*, Harmondsworth, Peregrine, 1976; en Torres, Rosa María "Sociedad de la información / Sociedad del conocimiento", *Universidad de Barcelona*, 21 de abril de 2005, http://www.ub.edu/prometheus21/articulos/obsciberprome/socinfsoccon.pdf

[130] *La informática se considera una gran amenaza para la privacidad porque permite una vigilancia omnipresente, bases de datos gigantescas y una veloz distribución de la información en el globo entero*. Nissenbaum, Helen, *Privacidad amenazada*, 1ª ed., trad. De Enrique Mercado, México, 2011, p.21.

[131] Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)

[132] "Gestión de riesgos, análisis y cuantificación", http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/4AnalisisycuantificaciondelRiesgo%28AR%29_es.pdf

Después de llevar a cabo un levantamiento de toda la información que se encuentra en posesión de un responsable y de todas aquellas partes relacionadas directa o indirectamente con éste, como es el caso de los empleados, recursos humanos externos, practicantes, servidores sociales, encargados[133] y terceros; debe procederse a una clasificación de la misma, es decir, del hiperónimo conocido como información habrá que categorizarse toda aquella de identifique o vuelva identificable a una persona física; posteriormente, atendiendo al nivel de riesgo de daño o discriminación que conlleva el tratamiento de esos datos, se determinará si estamos en presencia de datos considerados por la Ley como sensibles o no.

El resultado de todo este análisis, es el famoso inventario de datos, que más que un requerimiento legal, es un activo básico para el establecimiento de los procesos de seguridad de la información, que detallaremos más adelante.

El deber de seguridad, se encuentra establecido y relacionado con otros principios, en diferentes artículos de la Ley y su Reglamento[134], por ejemplo:

> ... *"Artículo 19*[135].- *Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.*
>
> *Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico."*

El cumplimiento cabal y estricto de este deber de seguridad es tan importante y trascendental, que, todo aquel responsable, encargado o tercero, que provoque una vulneración de seguridad, será acreedor a una sanción, la cual puede llegar incluso a ser de carácter penal.

---

[133] Se entiende por encargado a la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable, esta figura debe ser ajena a la organización del responsable, en términos del artículo 3º fracción IX, de la LFPDPPP y del artículo 49 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP).
[134] RLFPDPPP.
[135] LFPDPPP.

Es el RLFPDPPP, el que define de manera precisa, lo que se entiende por medidas de seguridad, su alcance, funciones, factores a tomar en cuenta para su determinación, acciones a seguir, actualizaciones, vulneraciones, comunicación de las vulneraciones y medidas correctivas en su capítulo III.

> *"Articulo 57. El responsable y, en su caso, el encargado deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Capítulo, con independencia del sistema de tratamiento. Se entenderá por medidas de seguridad para los efectos del presente Capítulo, el control o grupo de controles de seguridad para proteger los datos personales.*
>
> *Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular que la dispuesta en la Ley y el presente Reglamento."*

Del artículo 57 se desprende que la obligación de establecer y mantener todo tipo de medidas de seguridad, no sólo se limita a la figura del responsable sino a la del encargado, y aunque no lo menciona este artículo, hay que recordar que, en la mayoría de los casos, el tercero se convierte posteriormente en responsable y además de ello, el responsable al llevar a cabo la transferencia debe verificar, al menos por contrato, que el tercero también se encuentra en cumplimiento de la legislación en materia de protección de datos personales.

Lo anteriormente expuesto, conlleva una especie de cadena segura de manejo de información, que idealmente debe estar estandarizada en todas aquellas fases del ciclo de vida del dato, es decir, que de nada serviría que el responsable de los datos personales se encontrara en estricto cumplimiento si el encargado de los datos personales no está en la misma circunstancia, y por lo tanto, es éste último el eslabón vulnerable por donde puede haber fuga de información o acceso no autorizado a bases de datos personales, incluso sensibles.

Pensar en seguridad es pensar en minimización de riesgos, para conocer el riesgo es importante entender no sólo la naturaleza del dato sino la naturaleza de los medios de almacenamiento de la información y sus vulnerabilidades propias.

Cada soporte o medio de almacenamiento de la información es susceptible de sufrir tal o cual desastre natural o ser más apto para sufrir un ataque interno o externo; el papel es sensible al agua, a la humedad, al fuego, no es trazable, es fácil de traspapelar, es delicado para conservar; en el caso de los medios informáticos, son sensibles a otro tipo de circunstancias o ataques, si bien son trazables y su manipulación es fácil de identificar, es cierto que pueden ser objeto de ataques informáticos gestados incluso desde el interior de la empresa o ataques externos, a veces de países lejanos, son susceptibles al borrado accidental, a la copia no autorizada, a la extracción de información ilícita, al cifrado [136] que los pueda volver inaccesibles, en ocasiones pueden ser editables sin conocimiento del titular de la información, etc.

Hablando de medios magnéticos u otro tipo de cintas donde vivan datos relacionados con cámaras de video vigilancia, llamadas telefónicas, registros de voz, imágenes, datos, etc. de igual manera son vulnerables a otras condiciones meteorológicas, físicas, etc.

Hablar de medidas de seguridad es hablar de un sistema de seguridad, es decir, no de medidas y procesos aislados que no servirían de nada cuando de disminuir riesgos se trata, la seguridad de la información por naturaleza está basada en procesos, actividades y medios físicos que prevengan la modificación, alteración, destrucción, acceso o copia no autorizados, en pro de garantizar la famosa triada de la información: integridad, confidencialidad y disponibilidad[137], sea cual sea el formato en el que se haya la información y el soporte donde radica.

Para determinar correctamente las medidas de seguridad, el Reglamento de la Ley en su artículo 60, menciona los factores que debe tomar en cuenta para ello, los cuales se citan a continuación:

> *"Artículo 60. El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores:*

[136] Consultar: *https://www.certsuperior.com/Blog/que-es-el-cifrado-y-para-que-funciona-medida-de-seguridad-primordial-para-tu-empresa*
[137] Muñoz, Néstor "Qué es la triada CIA o CID", *https://es.linkedin.com/pulse/qué-es-la-triada-cia-o-cid-néstor-muñoz*

I. El riesgo inherente por tipo de dato personal;

II. La sensibilidad de los datos personales tratados;

III. El desarrollo tecnológico, y

IV. Las posibles consecuencias de una vulneración para los titulares.

De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:

I. El número de titulares;
II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;

III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y

IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable."

Estimar el nivel de riesgo de seguridad de cierta información catalogada como dato personal, se vuelve casi un cálculo matemático que además tome en cuenta los avances tecnológicos tanto para el tratamiento de la información como aquellas nuevas amenazas que se hayan desarrollado con motivo de éstos.

La delincuencia organizada ha migrado hacia el robo de información de manera creciente, por lo tanto, los mecanismos de acción se han vuelto cada vez más sofisticados, cada año existen nuevas tendencias en materia de *ciberdelitos*, los virus y troyanos que conocíamos a principios del año 2000, no se parecen en nada a los nuevos gusanos que se esparcen de manera casi instantánea utilizando

técnicas de ingeniería social para gestar un ataque de *ransomware*[138] y parar las actividades de servicios críticos como hospitales, transporte público, etc.

Además de conocer la calidad de la información que fluye por nuestra organización, el número de usuarios de quienes manejamos esa información, los medios en los que ésta reside, su potencial valor, etc. ahora es indispensable conocer las nuevas tendencias de seguridad[139] en función de los avances tecnológicos disponibles, las nuevas tendencias criminales y el grado de vulnerabilidad de nuestra empresa u organización ante estos nuevos ataques.

Desde la entrada en vigor de la Ley en 2010, la mayoría de los responsables y sus empleados se preguntaban acerca de una guía o recomendaciones que les ayudaran a cumplir cabalmente con sus obligaciones, es importante recordar que esta Ley le aplica tanto a personas físicas como a personas morales de carácter privado independientemente de su tamaño y estatus económico. Es de hace constar que aun y cuando el Capítulo III del Reglamento de diciembre de 2011, de las medidas de seguridad, en términos del artículo cuarto transitorio no entró en vigor hasta 18 meses después, las empresas debían empezar a aceitar motores en el tema a efecto de no ser sancionadas.

Cualquiera podría pensar que las grandes corporaciones, incluso desde antes de la entrada en vigor de la Ley, se encontraban en perfecta aptitud para enfrentar toda clase de vulneraciones en la seguridad de la información, sin embargo, a la fecha vemos que no es así, pues no se trata de una fuerte inversión de dinero en consultores o herramientas tecnológicas de vanguardia, sino en saber lo que guardamos y en función de ello aplicar las medidas idóneas, no es un aspecto cuantitativo sino cualitativo, asimismo, por desgracia, vemos que siete años después hay una gran cantidad de profesionales independientes que desconocen esta Ley o no se encuentran correctamente implicados o asesorados para su correcto cumplimiento.

Es por ello que la publicación de su reglamento vino a esclarecer un poco el tema, así como las recomendaciones emitidas por el INAI[140].

[138] http://cnnespanol.cnn.com/2017/05/15/que-es-un-virus-ransomware-y-como-actua/
[139] Sullivan, Brian et al. *Tendencias de Seguridad Cibernética en América Latina y el Caribe*, Estados Unidos de América, Symantec y la Organización de los Estados Americanos, 2014.
[140] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Las medidas de seguridad, en términos del Reglamento de la Ley, se clasifican de la siguiente manera:

	Referencia	Definición	Ejemplos
Medidas de seguridad administrativas	Art. 2 fracción V del RLFPDPPP	**Medidas de seguridad administrativas**: Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales.	En este rubro podemos encontrar todos aquellos procesos, procedimientos, políticas, normas internas, buenas prácticas documentadas, reglamentos internos, contratos y cláusulas de confidencialidad, contratos con encargados y de transferencia a terceros, capacitación, certificación, normas y estándares internacionales en materia de seguridad de la información como es el caso de la familia ISO 27000, la adhesión y certificación con base en los parámetros de autorregulación y todas aquellas acciones de carácter administrativo que permitan minimizar riesgos para la seguridad de la información.

Medidas de seguridad físicas	Art. 2 fracción VI del RLFPDPPP	**Medidas de seguridad físicas**: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para: a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información; b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones; c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y d) Garantizar la eliminación de datos de forma segura;	Dentro del marco de las medidas de seguridad física podemos encontrar un amplio catálogo de alternativas. Estas opciones pueden en sí mismas tener embebida alguna medida tecnológica o no. Podemos ir desde las medidas más rudimentarias y por todos conocidos como los cerrojos, candados, gavetas con seguridad, cajas fuertes, bloqueadores físicos de puertos USB, puertas de seguridad, cajas de seguridad en bancos, bóvedas subterráneas, hasta incluso la presencia de personal de seguridad controlando los accesos, hasta medidas mucho más sofisticadas como pueden ser las cámaras de video vigilancia, sensores de movimiento, cerraduras con reconocimiento biométrico, cerraduras inteligentes electrónicas, etc.

Medidas de seguridad técnicas	Art. 2 fracción VII del RLFPDPPP	**Medidas de seguridad técnicas:** Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que: a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados; b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.	Por último, tenemos a las medidas de seguridad que implican la aplicación de algún tipo de tecnología. Este tipo de mecanismos de seguridad, comúnmente sobrevalorados, tienen como finalidad el monitoreo, idealmente en tiempo real del flujo de la información así como el acceso que tienen a ella los usuarios con motivo de sus funciones para poder identificar a tiempo comportamientos atípicos que revelen una posible intrusión o alteración por parte de personas ajenas a la operación habitual y autorizada; dentro de las opciones más conocidas y económicas encontramos a los antivirus, anti programas espía, muros de fuego, bloqueo de cookies, y podemos ir subiendo el estándar de precio y sofisticación para llegar a soluciones de seguridad más robustas como los famosos DLP, o *Data Loss Prevention, o Data Leak Prevention*[141] (sistemas de prevención de pérdida de

[141] Consultar, *https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Data-Leak-*

			información), *sandbox* [142], hasta soluciones específicamente creadas para prevenir ataques de tipo *ransomware*. Sin olvidar nunca que el usuario suele ser la parte más débil del eslabón y para ello habrá que monitorear y controlar su actividad en los sistemas de la empresa, evitando que navegue por sitios inseguros, descargue aplicaciones y archivos no permitidos o actualizaciones apócrifas de programas de cómputo.

Como podemos observar, las opciones de los tres tipos de medidas exigidos por la Ley y su Reglamento, son diversas y mientras podamos demostrar que éstas son eficaces y obedecen a las circunstancias de nuestra organización, podremos dormir más tranquilos.

Así como existen diferentes tipos de medidas de seguridad, existen diferentes tipos de amenazas, las cuales en general se dividen en internas y externas, por desgracia en innumerables ocasiones ya sea por imprudencia o dolo, los empleados, colaboradores o miembros de la organización están implicados en las vulneraciones de seguridad de la empresa, y en otros más, se trata de ataques gestados desde fuera con amplio conocimiento del ADN de la compañía, como aquellos en los que un ex empleado rencoroso que conoce mejor que nadie los puntos débiles de la empresa, una vez fuera de ella organiza un ataque informático valiéndose del amplio conocimiento que tiene de las

Prevention.aspx

[142] Consultar, *http://blog.smartekh.com/sandbox-porque-paraque*

deficiencias de seguridad o abusando de la información a la que tuvo acceso.

Sorpresivamente los ataques externos no dirigidos son los menos frecuentes, es decir, la mayoría de los delincuentes, sobre todo los delincuentes informáticos, previo al incidente de seguridad, lo han planeado con meses y hasta años de anticipación estudiando a detalle cada movimiento, cada punto débil, cada brecha de seguridad para elevar la tasa de éxito de su encomienda y para dejar el menor número de huellas de su fechoría.

Lo que es un hecho innegable es el enorme compromiso que recae en el responsable que decide sobre el tratamiento de los datos personales de los titulares, respecto del correcto manejo de la información que se le ha confiado, pero en gran medida depende de las buenas prácticas que deben ser parte del día a día de cada empresa y profesionista en el mundo, al respecto el Dr. Rubén Vázquez en el libro intitulado "Seguridad y Defensa en el Ciberespacio[143]", en su capítulo respecto de las buenas prácticas comenta lo siguiente: "…es necesario que cada persona haga conciencia sobre su seguridad y la de su información, así como los riesgos y amenazas que pudiera enfrentar, de manera que pueda saber cómo reducir, evitar o transferir los riesgos existentes". Es así pues que las buenas prácticas, deben ser la pieza angular de nuestro pensamiento y comportamiento en el día a día para evitar exponernos a riesgos innecesarios o saber lidiar con ellos al momento de que por alguno de ellos nos veamos implicados en un incidente de seguridad.

Estimado lector, tal y como lo aprendimos hace más de diez años, la seguridad es un estado del espíritu, sustentado en la tranquilidad de saber qué es lo que tenemos, cuánto vale y sobre todo cómo lo protegemos; en este caso, la tan valiosa información.

La seguridad existe en la medida de la conciencia del riesgo.

CONCLUSIÓN DE LA TERCERA PARTE.

La seguridad es un asunto de todos y de cada día, la responsabilidad que conlleva el tratamiento de datos personales comienza con el buen uso y manejo de nuestra información y la de terceros, las empresas cada vez están más comprometidas con el cumplimiento de las reglas en

[143] Vázquez, Rubén, "Buenas prácticas para reducir los impactos de amenazas y riesgos de la información en el Ciberespacio", *Seguridad y Defensa en el Ciberespacio,* México, Centro de Estudios Superiores Navales, 2015, p. 248.

materia de tratamiento de información y con la aplicación de normas y medidas de seguridad.

Con la entrada en vigor del GDPR, el tema de autorregulación ha cobrado una nueva dimensión para los países europeos y los sujetos obligados, la elaboración de análisis de impacto en el tratamiento de los datos personales y los sellos de confianza son los temas que serán la agenda de 2018.

CONCLUSIONES

- La identidad digital comprende muchos más aspectos de los que se contemplan a primera vista: es nuestra auténtica huella virtual, todos los días vamos construyendo una historia y dejando estampa de nuestra actividad en el entorno digital, nuestros gustos, preferencias, miedos, rasgos de personalidad y en general, todo lo que nos individualiza y nos hace ser lo que somos; esa identidad, hoy en día se encuentra más expuesta que nunca, por lo tanto debemos ser particularmente cuidadosos con todo lo que dejamos ver de nuestra más profunda intimidad.

- Eso que comúnmente llamamos usurpación o robo de identidad no es más que el robo de identificadores, y, de hecho, atendiendo a los principios básicos conceptuales y dogmáticos el derecho penal, es un matiz más del fraude.

- El delito de usurpación de identidad no es una conducta ilícita aislada, es decir, que antes o después de su comisión hubo o habrá otros ilícitos, este delito puede ser únicamente cometido como medio preparatorio de otro delito, no debemos estudiar esta conducta de manera aislada, sino como un todo en conjunto con los hechos que le dieron origen y aquellos que pueden darse en un futuro, la investigación de los casos de usurpación de identidad no es cosa fácil ya que como hemos descrito, pueden ser casos asintomáticos cuyas consecuencias pueden descubrirse mucho tiempo después.

- Los cuerpos legislativos existentes y en vigor en los tres países, México, Estados Unidos y Francia, son bastantes y suficientes como para hacer frente a las amenazas a la identidad digital, debemos tener mucho cuidado de no caer en la trampa de la sobrerregulación, más bien, se requiere una correcta aplicación de la normativa, la instrumentación clara y pertinente de los casos, la obtención y preservación de evidencia digital idónea y por último, una correcta capacitación a las autoridades y cuerpos judiciales para hacer frente a los desafíos que conllevan los nuevos fenómenos de la sociedad de la información.

- México cuenta con laboratorios forenses a la altura de los más innovadores centros de investigación en materia forense informática del mundo, el trabajo que ha venido haciendo durante la última década la división científica de la Policía Federal, así como la Procuraduría General de la República, la Secretaría de Marina y la Secretaría de la Defensa debe

reconocerse y destacarse, pero sobre todo, se deben sumar esfuerzos en pro de la ciberseguridad nacional.

- El estudio de los casos de usurpación de identidad, así como la estrategia a seguir por parte de las autoridades gubernamentales a nivel internacional para combatirla, debe implicar el trabajo conjunto de sociedad civil, gobierno y empresas, asimismo deben ser grupos multidisciplinarios donde abogados y expertos en tecnología logren empatar sus ideas y necesidades, todas las posibles reformas a la legislación serán infructuosas si no logramos entender que bajo las leyes de la informática suceden cosas que a veces escapan del criterio clásico del jurista.

- La cooperación internacional es un elemento fundamental en la lucha contra el cibercrimen, en particular contra los ilícitos cometidos en contra de nuestra identidad digital; es imperativo que México ratifique el Convenio de Budapest y forme parte de todos los grupos de trabajo internacionales en materia de cibercrimen, ciberseguridad y control de identidades.

- Si el cibercrimen no conoce fronteras internacionales mucho menos respeta jurisdicciones estatales, este trabajo tiene como última propuesta, la integración de un cuerpo regulatorio de carácter federal en México, actualmente se está trabajando en la puesta en marcha de los acuerdos contenidos en la Estrategia Nacional de Ciberseguridad en este 2017, y se espera que estos esfuerzos rindan fruto en los próximos años.

BIBLIOGRAFÍA

AMUCHATEGUI REQUENA, G. et al., *Diccionario de derecho penal*, Oxford, México, 2012.

ARPAGIAN, Nicolas., *La cybersécurité*, Puf, Francia, 2010.

AZURMENDI ADARRAGA, Ana, *El Derecho a la propia imagen: su identidad y aproximación al derecho a la Información*, 2ª edición. Fundación Manuel Buendía / Universidad Iberoamericana. México 1998.

BARRAGÁN, Julia. *Informática y decisión jurídica*, 2ª edición, Fontamara, México, 2000.

BARRIOS GARRIDO, Gabriela, et al., *Internet y derecho en México*, Mc Graw Hill, México, 1998.

BECCARIA, *Tratado de los delitos y de las penas*, 18ª edición. Porrúa. México 2013.

BERNARD, G. et al., *Les institutions de la France*, Nathan, Francia, 2013.

CABRILLAC, Rémy., *Introduction générale au droit*, 11e éd., Dalloz, Alemania, 2015.

CÁMPOLI, Gabriel Andrés, *Derecho Penal Informático*, INACIPE, México, 2004.

CARR, Nicholas, *Superficiales ¿Qué está haciendo internet con nuestras mentes?*, 1ª edición. Taurus, México 2013.

CARVER, Charles S. et al., *Teorías de la personalidad*, 7ª edición, Pearson, México, 2014.

CCAZA ZAPANA, Joseph Emerson, *Diccionario elemental de criminalística, criminología y ciencias forenses*, 1ª edición, Editorial Flores, México, 2013.

CERVANTES, P. et al., *Internet negro. El lado oscuro de la red*, Paidós, México, 2016.

CHARPENEL, Y. et al., *Cyberciminalité. Droit pénal appliqué*, Economica, Francia, 2010.

CONSTANT, A. et al., *Réussir mémoires et thèses*, 4e éd., Gualino éditeur, Lextenso éditions, Francia, 2012.

D'AUZON, Olivier, *Les droits des internautes à l'ère de l'économie numérique*, Editions du Puits Fleuri, France 2013.

DAVARA RODRÍGUEZ, Miguel Ángel, *Delitos Informáticos,* Editorial Aranzadi, 1ª Edición, Madrid, 2017.

DAVARA RODRÍGUEZ, Miguel Ángel, *La protección de datos personales en el sector de las comunicaciones electrónicas*, Universidad Comillas, Madrid, 2003.

DE FAULTIER-TRAVERS, Sandra, *Aspects juridiques de l'information*, ESF Éditeur, Paris, 1991.

DE FELCOURT, Guy., *L'usurpation d'identité ou l'art de la fraudesur les données personnelles*, CNRS editions, Francia, 2011.

DE LA PARRA, Eduardo, *El Derecho a la propia imagen,* Tirant lo Blanch México, 2014.

DEBRAS, Jérôme., *Guide juridique des contrats en informatique*, 2e éd., Eni editions, Francia, 2015.

DESGENS-PASANAU, Guillaume., *La protection des données personnelles*, 2e éd., LexisNexis, Francia, 2015.

DEYRA, Michel., *L´essentiel de la note de synthèse*, 8e éd., Gualino éditeur, Lextenso éditions, Francia, 2015.

FABRE-MAGNAN, Muriel. et al., *Que sais-je? Introduction au droit*, Puf, Francia, 2016.

FAUVARQUE-COSSON, B. et al., *Le cloud computing l'informatique en nuage*, Société de législation comparée, Francia, 2014.

FÉRAL SCHUHL, Christiane, *Cyberdroit*, 3a edición, Dalloz, París, 2002.

FERRY, J. et al., *Cybercriminalité. Défi mundial*, 2e éd., Economica, Francia, 2009.

FILIOL, Éric y RICHARD, Philippe, Cyber Criminalité, enquête sur les mafias qui envahissent le web", Dunod, Paris, 2006.

FILLOUX, Jean-Claude, "La personalidad", Publicaciones Cruz O., S.A., 1ª edición, México, 1992.

FOREST, David, "Droit des données personnelles", Gualino, París, 2011.

FOREST, David., *Droit en action. Droit des données personnelles*, Gualino éditeur, Lextenso éditions, Francia, 2011.

FRANKL, Viktor, *El hombre en busca de sentido*, Herder Editorial, Barcelona, 2015.

GIROT, J. et al., *Le harcèlement numérique*, Dalloz, Francia, 2005.

GUINCHARD, S. et al., *Lexique des termes juridiques*, 22e éd., Dalloz, Lyon, 2014.

H. CAMARA DE DIPUTADOS. et al., *Protección de datos personales. Compendio de lecturas y legislación*, Tiro corto editores, México, 2010.

HOFFMAN Reid et al., "El mejor negocio eres tú", 1ª edición. Conecta. México, 2013.

ITEANU, Oliver., *L'identité numérique en question*, Eyrolles, Francia, 2008.

ITEANU, Oliver., *Quand le digital défie l´état de droit*, Eyrolles, Francia, 2016.

JOLY-PASSANT, Elisabeth., *L´écrit confronté aux nouvelles technologie*s, Librairie Générale de Droit et de Jurisprudence, Francia, 2006.

KAPLAN, Daniel et al., *Informatique, libertés, identités*, Éditions FyP, France, 2010.

LACOUR STÉPHANIE et al., *La securité aujourd'hui dans la societé de l'information*,

L'Harmattan, Paris, 2007

LATREILLE, Antoine *Numérisation* Lex Electronica, 2017

LAFFAIRE, Marie-Laure., *Protection de données à caractère personnel*, Éditions d'Organisation, Francia, 2005.

LESSIG, Lawrence, *Code and other Laws of Cyberspace*, Basic Books, EUA, 1999.

LIRA ARTEAGA, Óscar Manuel, *Cibercriminalidad. Fundamentos de investigación en México*, 1ª. Ed., INACIPE, 2010.

LIRA ARTEAGA, Oscar Manuel., *Cibercriminalidad. Fundamentos de investigación en México*, Instituto Nacional de Ciencias Penales, México, 2010.

LLANO CIFUENTES, Carlos, *Viaje al Centro del hombre*, Ediciones Rialp, Madrid, 2010

LONG, J., *Google Hacking, Mettez vos données sensibles à l'abri des moteurs de recherches*, Dunod, París, 2005.

MAGAÑA RUFINO, José Manuel, *Curso de derechos de autor en México*, Novum, México, 2013.

MAGAÑA RUFINO, José Manuel, *Derecho de la propiedad industrial en México*, Porrúa, Universidad Panamericana, México, 2011.

MANARA, Cédric., *Réseaux sociaux: 101 questions juridiques*, Dianteino, Francia, 2013.
MANARÁ, Cédric et al, *Réseaux sociaux: 101 questions juridiques*, Diateino, France, 2013.

MARTIN Y MARTIN, Ricardo M., *Delincuencia informática y Derecho Penal*, Edisofer, Madrid, 2001

MATTATIA, Fabrice., *Internet et les réseaux sociaux: que dit la loi?*, Eyrolles, Francia, 2015.

MATTATIA, Fabrice., *Traitement des données personnelles. Le guide juridique*. Eyrolles, Francia, 2013.

MEJÁN, Luis Manuel C. *El Derecho a la Intimidad y la Informática*, 2ª edición. Porrúa, México, 1996

MENDOZA BEIVIDE, Ada Patricia, *Psiquiatría para criminólogos y criminología para psiquiatras*, Trillas, México, 2006.

MUÑOZ MACHADO, Santiago, *La regulación de la red, Poder y Derecho en Internet*, Taurus, Madrid, España, 2000.

NAVA GARCÉS, Alberto Enrique et al., *El derecho en la era digital*, 1ª edición, Porrúa, México, 2013.

NAVA GARCÉS, Alberto Enrique, *Delitos informáticos*, 2ª edición, Porrúa, México, 2007.

NAVA GARCÉS, Alberto Enrique, *La prueba informática en materia penal*, 1ª edición, Porrúa, México, 2011.

NAVARRO, Joe., *Personalidades peligrosas*, Ediciones B, México, 2016.

NISSENBAUM, Helen, *Privacidad amenazada. Tecnología, política y la integridad de la vida social*, 1ª edición, Océano, México, 2011.

ORTÍZ BAHENA, M. et al., *Ley de la Propiedad Industrial comentada por la asociación mexicana para la protección de la propiedad intelectual (AMPPI)*, Porrúa, México, 2015.

PAILLER, Ludovic, *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Larcier, Bélgica, 2012.

PARKER, Donn B., *Crime by computer*, Charles Scribner's sons, Nueva York, EUA, 1976.

QUINTANILLA MADERO, Beatriz., *Personalidad madura. Temperamento y carácter*, Publicaciones cruz o, Universidad Panamericana, México, 2008.

RANGEL ORTIZ, Horacio., *La observancia de los derechos de propiedad intelectual. Jurisprudencia*, Organización Mundial de la Propiedad Intelectual, Suiza.

RENAULT-BRAHINSKY, Corinne, *L'essentiel de la procédure pénale*, 13ª edición, Gualino, París, 2013.

REYES KRAFFT, Alfredo Alejandro, *La firma electrónica y las entidades de certificación*, Porrúa, México, 2003.

REYES KRAFFT, Alfredo Alejandro., *La firma electrónica y las entidades de certificación*, Porrúa, México, 2008.

REYES KRAFFT, Alfredo Alejandro. et al., *Seguridad y defensa en el ciberespacio*, Centro de Estudios Superiores Navales, Secretaría de Marina, México, 2015.

RODRIGUEZ, Philippe., *La révolution blockchain*, Dunod, Francia, 2017.

ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Comares, Granada, España, 2002.

SCHULTZ, Duane P. et al., *Teorías de la personalidad*, Cengage Learning, México, 2010.

TELLEZ CARVAJAL, E. et al., *Derecho y TIC. Vertientes actuales*, Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, México, 2016.

TENORIO CUETO, G. et al., *Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares*, Porrúa, Universidad Panamericana, México, 2012.

UROSA RAMÍREZ, Gerardo Armando., *Guía de estudio de derecho penal*. Parte general, Porrúa, México, 2009.

TEXTOS LEGISLATIVOS Y REGLAMENTARIOS

- Constitución Política de los Estados Unidos Mexicanos, 15 de septiembre de 2017.
- Código Civil Federal, 24 de diciembre de 2013.
- Código de Comercio, 2 de mayo de 2017.
- Código Penal Federal, 17 de noviembre de 2017.
- Código Federal de Procedimientos Civiles, 9 de abril de 2012.
- Código Nacional de Procedimientos Penales, 17 de junio de 2016.
- Ley de Firma Electrónica Avanzada, 11 de enero de 2012.
- Ley de la Propiedad Industrial, 1 de junio de 2016.
- Ley Federal de Transparencia y Acceso a la Información Pública, 27 de enero de 2017.
- Ley Federal del Derecho de Autor, 13 de enero del 2016.
- Ley Federal de Protección al Consumidor, 26 de junio de 2017.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 5 de julio de 2010.
- Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal, 19 de mayo de 2006.
- Disposiciones de Carácter General Aplicables a las Instituciones de Crédito, 11 de septiembre de 2017.
- Reglamento de la Ley de Firma Electrónica Avanzada, 21 de marzo de 2014.
- Reglamento de la Ley de Propiedad Industrial, 16 de diciembre de 2016.
- Reglamento de la Ley del Derecho de Autor, 14 de septiembre de 2005.
- Reglamento de la Ley Federal de Protección al Consumidor, 3 de agosto de 2006.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 21 de diciembre de 2011.
- Code Civil

- Code Penal
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
- Digital Millennium Copyright Act

Université Paris-Saclay
Faculté Jean Monet, Université Paris Sud
54, Boulevard Desgranges
92330 SCEAUX

Actividad	GDPR	LFPDPPP	RLFPDPPP
Asignar un responsable del Departamento de Datos Personales (CPO)	27	30	
Asignar al DPO un rol independiente	37, 38	30	
Concientización y compromiso de todas las áreas de la organización en el tema de privacidad		30	48
Descripción de puesto	39		61, 57
Elaborar un Análisis de Riesgos	24,39	19	
Tener un inventario de datos personales	30		61
Clasificar debidamente la información			2 V
Mantener un inventario de medidas administrativas de control de transferencias nacionales e internacionales de datos personales	45, 46,49		68, 69, 71, 73, 74, 75.
Utilizar los mecanismos de autorregulación aprobados por la		43, 44	79, 80, 81, 82, 83, 84, 85, 86

autoridad como políticas corporativas de transferencia de datos personales			
Transferir datos personales en los casos exceptuados por Ley	45,49,48	8, 37	68, 70
Contar con una política de privacidad	5,24,91		47, 48, 52, 80
Documentar las bases legales de tratamiento de datos personales	6,9,10		7,10, 30, 36, 37, 43,
Contar con procesos de obtención de datos sensibles	9	9, 16	15, 17, 56,
Contar con procesos de obtención de datos de menores	8,12	19	89
Contar con procedimientos para mantener la calidad de la información	5		36
Contar con procedimientos para identificar los datos personales	89		60, 61
Contar con políticas para el control del tratamiento automatizado de datos	12, 22		
Contar con políticas para el control del tratamiento secundario de datos (finalidades secundarias)	6, 13, 14		
Contar con políticas para la	6, 7, 8	33, 63, 64	47, 48, 52, 62,

obtención del consentimiento del tratamiento de datos			80
Integrar políticas de privacidad en el proceso de conservación de los datos	5	33, 63, 64	47, 48, 52, 62, 80
Integrar políticas de privacidad en el proceso de marketing y publicidad	21	33, 63, 64	47, 48, 52
Integrar políticas de privacidad en el proceso de social media	8	33, 63, 64	47, 48, 52
Integrar políticas de privacidad en el proceso de investigación	21, 89	33, 63, 64	47, 48,52
Entrenamiento en materia de privacidad	39	39	2
Integrar el tópico de privacidad de datos dentro del análisis de riesgo de seguridad de la información	32	33	57
Integrar el tópico de privacidad de datos dentro de la política de seguridad	5, 32	33	57
Contar con medidas de seguridad técnicas	32	19	57
Medidas para cifrar datos personales	32	19	57, 61, 62
Medidas para restringir el acceso a	32		57, 61, 62

los datos			
Realizar pruebas periódicas de la seguridad de los datos	32	19	61, 62
Mantener registros de los procesos de privacidad que tengan que ver con terceros	28, 32	36, 37	67,68,69,70,71, 72, 73, 74, 75, 76
Contratos con encargados o procesadores de datos	28, 29	3	49, 50, 51,53, 54, 55
Verificar cumplimiento de protección de datos personales con encargados	28	3	49, 50, 51,53, 54, 55
Contar con avisos de privacidad	8, 13, 14	3,15, 16, 17	23,24,25,26, 27, 28, 29, 30, 31
Contar con avisos de privacidad en cada punto donde se colectan datos personales	13, 14,21	3,15, 16, 17	23,24,25,26, 27, 28, 29, 30, 31
Procesos de ejercicio de derechos ARCO	15, 16, 19, 7, 18, 21	28,29,30,31, 32,33,34,35	23,24,25,26, 27, 28, 29, 30, 31
Procesos de portabilidad de datos	20		
Privacy by Design	25		
PIA	5, 6, 25, 35, 36		
Procedimiento de respuesta a	33, 34	20	65, 66

incidentes de seguridad			
Protocolo de notificación de brecha de seguridad	12, 33, 34	20	63,64,65,66
Registros de incidentes de seguridad	33	20	63,64,65,66
Parámetros de Autorregulación	25, 39	44	47
Documentos que avalen el cumplimiento y la rendición de cuentas	5, 24		47, 48, 80
Identificación de normas	39		

ANEXO II. ANTECEDENTES HISTÓRICOS Y EVOLUCIÓN DE LA REGULACIÓN NORTEAMERICANA EN MATERIA DE PRIVACIDAD Y PROTECCIÓN DE DATOS.

En este reporte, se va a comentar acerca de la evolución que ha tenido la regulación de los E.E.U.U. a través de los años, así como los criterios que se han publicado de su Corte. Es importante mencionar que dicha regulación, no surgió como en Europa, ya que en los E.E.U.U. siguen el sistema anglosajón que se fue ahondando cada año con los casos que se presentaban, y que los fue orillando a ir regulando con el tiempo.

De este trabajo de investigación, se desprende que su regulación no está contenida en un solo cuerpo, sino que se puede consultar en leyes de distintos temas, así como de varios precedentes. Además, es importante mencionar que la privacidad desde sus orígenes se vinculó con la dignidad y reputación de las personas. Lo anterior se confirmará en los siguientes reportes:

Época Colonial[144]

Era complicado el respetar la privacidad de las personas, pues viviendo en pueblos pequeños, todos los habitantes de un pueblo sabían acerca de la vida privada de sus vecinos aun así había cierta protección tanto en la ley como en los precedentes:

Regulación de Common Law	Precedentes
Se castigaba el "*eavesdropping*" o espiar a terceros en sus hogares para calumniar.	En 1488, surge el caso Seymane, donde el pronunciamiento judicial determinó que "*El hogar de cada individuo es para este último como su castillo y fortaleza*", refiriéndose a la inmunidad que una persona debe tener en su hogar.

Época de la Revolución[145]

La cuestión en privacidad giraba en torno a buscar la libertad en contra del entrometimiento del gobierno a través de mandos de asistencia o "*writs of assistance*", donde se autorizaba a hacer búsquedas y confiscamiento de bienes sin fundamento alguno, que impulso a las siguientes enmiendas:

[144] Daniel J. Solove, A Brief History of Information Privacy Law. The George Washington University Law School. http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications, consultado el 17 de Julio de 2017.
[145] Ídem

Enmienda	Contenido
Tercera	Protege a la privacidad en cuanto a que prohíbe al gobierno de mandar a soldados a residir en casas de individuos sin su consentimiento.
Cuarta	Protege el derecho de las personas de estar seguras en su persona, hogar, documentos y efectos en contra de cualquier búsqueda o confiscamiento de autoridades sin autorización judicial.

Siglo XIX[146]

Hubo varios factores que detonaron la necesidad de regular en materia de privacidad:

Factor	Resultado
Censos	Muchas de las preguntas en los censos eran acerca de detalles muy personales, además se publicaban en plazas, pero se detuvo en 1870, debido a leyes que exigían proteger la confidencialidad de datos obtenidos en censos
Servicio Postal	Había problemas de intercepciones de cartas, por lo que hasta 1782 el Congreso aprobó una ley donde el correo ajeno no se debía abrir. • En 1825 el Congreso estableció un estatuto donde cualquier intercepción de una carta o un escrito, ya sea para evitar que llegue a su destino, acceder a la información o destruirla, podía ser sancionada con multas o hasta aprisionamiento. • Esto se extendía hasta autoridades gracias a la cuarta enmienda
Telégrafo	Después de su invento en 1844, muchas comunicaciones eran interceptadas para planes de batalla durante la Guerra Civil. Resultó en muchas quejas circuladas en periódicos famosos que los impulsó a realizar un proyecto de ley de proteger la privacidad pero quedó abandonado. • Provocó que las Cortes rechazaran solicitudes *supoena* ya que vulneraban la confidencialidad de su contenido. Esto gracias a que por analogía relacionaron al telegrama con una carta
Criterios de la Corte sobre la Privacidad del Cuerpo	1. **Union Pacific Railway v. Botsford.-** La Suprema Corte decidió que no podía obligar a la demandante a someterse a una examinación de cuerpo para analizar los daños que su cuerpo había recibido por el mal diseño de un remolque, como el juez Gray comentó: *"el obligar a alguien… a ser sometido a un estudio de cuerpo ante un extraño sin autorización es una indignación, un asalto y una infracción*".

[146] Patrick o. Callahan, The Oxford Encyclopedia of American Political & Legal History, Oxford University https://books.google.com.mx/books?id=QSnQ5NPtoOUC&pg=PA75&lpg=PA75&dq=privacy+case+laws+nineteenth+century&source=bl&ots=OrU2Ck2Hl0&sig=ijf1cHPCVAIM59lg1oJp1JQrSEI&hl=es&sa=X&ved=0ahUKEwj6_6yVsZHVAhWBSyYKHdVmAUcQ6AEIUzAG#v=onepage&q=privacy%20case%20laws%20nineteenth%20century&f=false

	2. **De May V. Roberts**[147].- La Suprema Corte decidió que el consentimiento de una persona para decidir sobre su propio cuerpo debe ser expresamente y con antes estar informado. Esto debido a que Roberts demandó a De May, ya que llevó a su asistente Scattergood para examinar su cuerpo, sin haberle informado que este último no era doctor.
Aportación de Warren y Brandeis[148]	Escriben un artículo llamado **"El Derecho a la Privacidad"** (The Right to Privacy), publicado en 1890, ya que no había como tal una acción legal para proteger los derechos de privacidad. Propusieron **4 limitaciones con el fin de definir el derecho a la privacidad** **a.** No se prohíben las publicaciones que sean de interés público. **b.** No se prohíbe la comunicación de cualquier asunto, pero cuando se haga una publicación de algo, se debe cumplir con las disposiciones de la ley en contra de la difamación **c.** Por la simple publicación oral y sin daño directo, no se daría un remedio por ley. **d.** El derecho a la privacidad cesan el momento que un individuo publica ciertos hechos o consiente para ello. **La Suprema Corte de Georgia reconoció 3 años después con el caso Pavesich v. New England Life Ins. Co**., donde la Corte condenó a la Aseguradora New Ingland Life Ins. Co., por publicar el nombre, retrato y un testimonio falso en un periódico sin el consentimiento del demandante. *"One who desires to live a life of partial seclusion has a right to choose the times, places, and manner in which and at which he will submit himself to the public gaze. Subject to the limitation above referred to, the body of a person cannot be put on exhibition at any time or at any place without his consent…. It therefore follows from what has been said that a violation of the right of privacy is a direct invasion of a legal right of the individual".*[149]

Siglo XX: 1930-1960[150]

[147] DeMay v. Roberts, Casebiefs, consultado en http://www.casebriefs.com/blog/law/evidence/evidence-keyed-to-mueller/privileges/de-may-v-roberts/

[148] Daniel J. Solove, A Brief History of Information Privacy Law. The George Washington University Law School. http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications, consultado el 17 de Julio de 2017.

[149] PAVESICH v. NEW ENGLAND LIFE INS. CO. En: http://rightofpublicity.com/pdf/cases/pavesich.pdf Consultado el 18 de julio de 2017

[150] Daniel J. Solove, A Brief History of Information Privacy Law. The George Washington University Law School. http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications, consultado el 17 de Julio de 2017.

Gracias a la aportación de Warren y Brandeis, y que la Suprema de Corte de Georgia haya emitido su resolución de **Pavesich v. New England Life Ins. Co**., esto creó un precedente desde 1905, resultando que para 1939 muchas cortes siguieron el sentido de esta resolución, y después se desarrollaron las siguientes responsabilidades (Torts):

Restatement of Torts [151] **, Capítulo IV**	**Comentarios**
Intrusion Upon Seclusion	*"One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."* Quien intencionalmente se entrometa por cualquier medio a los asuntos privados de otros, será responsable de la invasión de la ´privacidad del otro, en caso de que dicha invasión sea razonablemente ofensivo.
Public Disclosure of Private Facts	*!One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."* Quien de publicidad a un asunto concerniente a la vida privada de otro será responsable en la medida que sea ofensivo y no sea legítimo su conocimiento al público.
False Light	*"One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if* *(a) the false light in which the other was placed would be highly offensive to a reasonable person, and* *(b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed."* Quien de publicidad a un asunto concerniente a otra persona que la coloque ante el público sobre asuntos falsos, está sujeto a responsabilidad por haber invadido la privacidad si es altamente ofensivo y además que este haya sabido acerca de la falsedad de lo publicado.
Appropriation	*"One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy"* Quien se apropie para beneficio propio del nombre o similar de otra persona, es responsable de la invasión de su privacidad.

[151] Arthur L. Goodhart, Restatement of the Law of Torts, University of Pennsylvania, 1943. http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9307&context=penn_law_review

También empezó a surgir la regulación en materia de privacidad de manera segmentada, como sucedió con la Ley Federal de Comunicaciones (Federal Communciations Act) de 1934, donde añadieron la sección 605, una disposición que sancionada las intervenciones de comunicaciones privadas.[152]

Siglo XX: 1960-1980

Con los antecedentes de privacidad, así como la creación de la ley de Derechos Civiles, la protección a la privacidad se desarrolló más a fondo en materia de investigaciones criminales, así como en el sistema financiero:

Ley/ Precedente	Comentarios
Mapp V. Ohio	En 1961, la Suprema Corte decidió que en todos los procedimientos de índole penal, la evidencia que se obtuviera en contra de lo dispuesta en la cuarta enmienda, no podía ser utilizado como evidencia en juicios.
Katz v. United States	En 1967, Katz demandó al gobierno por haber interferido una llamada telefónica que tuvo en una cabina telefónica. La Suprema Corte decidió que lo que una persona conscientemente expone al público, aún cuando sea en su casa o en una oficina, no se puede proteger bajo lo dispuesto por la Cuarta Enmienda, sin embargo; lo que este busque mantener en privado, aun cuando esté en un área pública, puede ser constitucionalmente protegido. De aquí surge el análisis de la expectativa razonable de privacidad, que pregunta si: • Una persona exhibe dicha expectativa y • Que la expectativa es la que la sociedad considere razonable
Título III de la Ley de Control a la Delincuencia de 1968	Con Katz, añadieron el título III (Omnibus Crime and Control Act) para proteger a los individuos en contra de las intervenciones, se limitaba a comunicaciones auriculares, o sea que estaban excluidas las vigilancias visuales y otras formas de comunicación electrónica.
El Derecho	La Corte reconoció que la Constitución protegía indirectamente una "zona de privacidad"

[152] Sección 605 De la Ley Federal de Comunciaciones de 1934: *"no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person."*

Constitucional a la Privacidad: Griswold v. Connecticut	la cual salvaguardaba la autonomía individual, concerniente a la toma de decisiones en el propio cuerpo. Es en el caso de **Griswold v. Connecticut** donde se decidió que el gobierno no podía prohibir anticonceptivos, ya que una mujer tenía el derecho de decidir en su propio cuerpo si deseaba tener hijos o no.
Whalen v. Roe	En 1977, la Corte decidió que la "constitucionalidad" en la "zona de privacidad" protege dos tipos de intereses: a. La independencia al poder realizar decisiones personales b. El interés individual de poder evitar la revelación de asuntos personales.
Privacy Act of 1974	Después de tantos eventos decidieron emitir una Ley de Privacidad, esta regulaba acerca de la recabación y el uso de datos que utilizaban las agencias de gobierno federales, y también contemplaba el derecho de los individuos de poder acceder y corregir sus datos personales. Aun cuando fue una gran aportación al no aplicar al sector privado ni a dependencias de gobierno locales
Family Educational Rights and Privacy Act of 1974	También conocida como la Enmienda Buckley, encargada de la protección a la confidencialidad de la información académica de los estudiantes. Provee los mecanismos para hacer valer estos derechos de privacidad y las excepciones correspondientes. Su cumplimiento es obligatorio para instituciones educativas solamente.
Foreign Intelligence Surveillance Act of 1978	Se creó regulación para la vigilancia electrónica, esta es permitida, así como las búsquedas en secreto cuando haya una orden judicial de por medio, y es para poder utilizar dicha información en procedimientos penales. , solo se puede conceder la orden si hay causa suficiente para suponer que se puede conseguir evidencia de un crimen relacionado
Fair Credit Reporting Act of 1970	Al principio, todos en un pueblo sabían acerca del estado financiero de otros, se podía saber acerca de datos financieros con preguntar a la sociedad, pero en el siglo XX esto ya no era factible, por lo que empezaron a realizar registros para mantener documentados los estados financieros de las persona de manera muy detallada, que incluyen deudas, declaración de bancarrota, procedimientos judiciales e hipotecas, por ello surge la ley para dar un poco de protección a los titulares de los datos: • Pueden acceder a sus registros, solicitar modificaciones • Lomita la man era en como peen ser revelados estos registros • No protege a los usuarios de "Difamación, Invasión de privacidad o negligencia", a menos que se demuestre la mala fe de querer causar dicho daño al usuario.
Bank Secrecy	Para investigaciones judiciales y policiales en contra de delitos de cuello blanco, se le

Act of 1970	obliga a los bancos a elaborar reportes y registros de sus usuarios, que incluyen datos de identificación. No podían revelar los datos a un tercero, sólo mediante orden judicial.
United States v. Miller In 1976	La Corte afirmó que si una autoridad obtiene datos de una persona, debido a una orden judicial, es legal y los individuos no pueden reclamar acciones con base en la Cuarta Enmienda.
Right to Financial Privacy Act of 1978	Se delimita más el acceso por parte de las autoridades, se hicieron más formalidades y además se añadió que las autoridades debían informar previamente de ello al usuario investigado.

Siglo XX: Década de los 80´s

En los 80s, se desarrolló el concepto de la expectativa razonable de privacidad

Ley/ Precedente	Comentarios
Florida v. Riley 1988[153]	La Corte determinó que no se había respetado la expectativa razonable de privacidad, cuando la policía voló sobre ella en un helicóptero, cuando estaban tratando de obtener evidencia acerca de si Riley cultivaba marihuana en su casa.
California v. Greenwood 1988[154]	La policía estaba investigando a Billy Greenwood pues tenían sospechas de que vendía drogas, no tenían suficiente evidencia por lo que buscaron en su basura y encontraron respuesta. En el procedimiento, la Corte determine que la razonable expectativa de privacidad no se puede respetar en la basura de las personas, pues cualquier ser puede acceder a ellas, además que se coloca en dicho sitio para que un tercero se la lleve.
New Jersey, v. T.L.O 1985[155]	T.L.O, vendía marihuana en su escuela, la descubren debido a que el director le investigó su bolsa. Ella alegó que la forma en que obtuvieron la evidencia no era legal, el caso llega hasta la Suprema Corte, donde esta determinó que sí lo es, ya que la expectativa razonable de privacidad está reducida en la escuela
Privacy Protection Act	La ley protege en contra del confiscamiento de cualquier obra material obtenida por una persona que se crea que esta última tiene la intención de publicarla, se necesita una subpoena o requerimiento para obtenerla y en el requerimiento la persona se puede oponer, todo sin que haya autoridades entrometiéndose en lugares privados.
Cable	En una sección protege la privacidad de los usuarios, pues obliga a las empresas de

[153] https://www.oyez.org/cases/1988/87-764
[154] https://www.oyez.org/cases/1987/86-684
[155] http://www.uscourts.gov/about-federal-courts/educational-resources/supreme-court-landmarks/new-jersey-v-tlo-podcast

Communications Policy Act of 1984	cable a no revelar a cualquiera la conducta de un usuario en los diversos canales, además de que se les debe de notificar a los usuarios de la recolección de sus datos asó como el uso.
Employee Polygraph Protection Act of 1988	Protege a los empleados y candidatos, prohíbe a los patrones de utilizar detectores de mentiras en sus empleados para indagar sobre asuntos probados, si puede ser utilizado en caso de querer investigar un robo, accidente, o espionaje de la empresa
Video Privacy Protection Act of 1988	Prohíbe que este tipo de empresas revele a terceros las películas que sus usuarios hayan rentado.
Electronic Communications Privacy Act of 1986	Se reforma la de 1968, se expandió para enfocarse en el uso de computadoras, por lo que la protección en contra de intercepción de comunicaciones también ahora las incluía.
OECD Guidelines and International Privacy[156]	Se crearon los lineamientos de protección d la información en material de privacidad para los miembros de la OCDE en 1980. Contenía los siguientes 8 principios que se debían cumplir para comercializar con miembros de la OCDE • Limitación de la colección.- Se debe recolectar solo la indispensable para trabajar y tener el consentimiento del titular • Calidad.- debe ser relevante y correcta. • Especificación del fin.- Se debe establecer desde que se recaban los datos y se limita solo a eso • Limitación de uso.- Solo se usa para lo determinado en un principio • Medidas de seguridad • Principio de transparencia.- los titulares deben ser informados acerca de las prácticas y políticas de quienes manejen sus datos • Participación del Titular.- Tienen derecho a contactar al responsable, y de modificar errores en sus datos • Responsabilidad.- Quienes manejen estos datos se responsabilizan por ello

[156] http://www.oecd.org/sti/ieconomy/15590267.pdf

Siglo XX: Década de los 90´s y la Llegada del Internet para cuestiones comerciales

Ahora no solo había computadoras que almacenaban mucha información, sino que el internet abrió más comunicaciones, así como nuevas formas de recabar información, como son la utilización de las tecnologías como las cookies, web bugs y más que se utilizaron con fines de marketing en el internet.

Ley/ Precedente	Comentarios
Telephone Consumer Protection Act of 1991	Permite que los usuarios hagan una solicitud para que vendedores por teléfono no los vuelvan a contactar, y si lo hacen, se puede demandar por responsabilidad.
Driver's Privacy Protection Act of 1994	Por muchos años, los estados vendían los registros de manejo (MVR) de los usuarios para los de marketing y vender mejor los planes y seguros de vehículos. El MVR[157], incluye información acerca de la licencia de manejar, antecedentes, y datos personales del Usuario. Esta Ley protegió la privacidad de los conductores, donde primero se necesita el consentimiento antes de poder revelar esa información.
Health Insurance Portability and Accountability Act of 1996[158]	Protegía la privacidad de los antecedentes médicos de pacientes, y que solamente con el consentimiento del usuario se podrán compartir sus datos para cuestiones de revelar dichos datos a aseguradoras, igual para las autoridades, necesitan obtenerla a través de una *subpoena* donde el paciente puede oponerse. Con base en los principios de esta ley, las siguientes regulaciones surgieron: a. **Los Estándares para la Privacidad de la Información de Salud Individualmente Identificable**, se aplican a la recopilación y uso de información de salud protegida. b. **Los Estándares de Seguridad para la Protección de la Información Médica Electrónica Protegida.** c. **Los Estándares para Transacciones Electrónicas**, se aplican a la transmisión electrónica de datos médicos.

[157] http://www.dmv.org/insurance/motor-vehicle-report.php
[158] Consultada en http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx, el 20 de julio de 2017.

	d. **La Regla de Notificación de Violación de Seguridad**, requiere que las entidades obligadas den un aviso cuando existan violaciones de uso de información de salud.
Children's Online Privacy Protection Act of 1998	Regula sobre la recolección de datos personales de los menores en internet, solo aplica para menores de 13 años, y en la ley se menciona que se necesita el consentimiento de los padres. Y esta ley solo aplica a sitios web que sean para un público de menores de 13 años, o un sitio que sepa que puede recabar dichos datos.
The Gramm-Leach-Bliley Act of 1999	Permite a instituciones financieras que entre sus diferentes ramas o afiliadas se pueden compartir libremente datos personales, siempre que se informe de esto a los usuarios, pero si la quieren compartir con terceros, los usuarios tienen derecho de oponerse a ello. El problema es que el oponerse "opt-out", pocos usuarios lo ejercieron ya que en un principio, se redactaban los avisos de privacidad de manera muy complicada.
Kevin Mitnick, 1999[159]	Por este hacker, se le dio relevancia a combatir crímenes realizados a través del internet, este individuo realizó accesos ilícitos, fraudes e intercepción de comunicaciones robando millones de dólares.

Siglo XXI: La Privacidad después del Terrorismo[160]

Después del 11 de septiembre del 2001, hubo una necesidad política muy fuerte de tener nuevas medidas de seguridad que justificó en ciertos casos la invasión de la privacidad

Ley/ Precedente	Comentarios
USA Patriot Act of 2001	Permitió la intervención de comunicaciones en correos electrónicos y direcciones IP. Además expandió su ámbito de aplicación, donde debían demostrar el propósito de la investigación, pero ahora es un propósito significativo en la investigación, por lo que es permitido si el sector de inteligencia necesita investigar. Surgió para contrarrestar esto, el "Muro" para protegerse de investigaciones, pero la Corte determinó que la palabra "Significativo" era la que permitía al gobierno el seguir investigando, además que la Seguridad Nacional permeaba más en este caso.[161]

[159] : Kevin Mitnick Case: 1999 - No Bail, No Computer, Hacker Pleads Guilty - Computers, Hacking, Access, and Unauthorized - JRank Articles http://law.jrank.org/pages/3791/Kevin-Mitnick-Case-1999.html#ixzz4nU7bPxd9 http://law.justia.com/cases/federal/appellate-courts/F3/145/1342/470528/

[160] Colleen Walsh, THE LAW BEFORE AND AFTER 9/11, Harvard Gazette. Consultado el 19 de Julio de 2017.http://news.harvard.edu/gazette/story/2011/09/the-law-before-and-after-911/

[161] Logan Cedric, THE FISA WALL AND FEDERAL INVESTIGATIONS, NYU Law, Consultado el 20 de Julio de

The National Do-Not-Call Registry	El registro creado por la Comisión Federal de Comercio y la Comisión Federal de Comunicaciones crearon este registro, donde cada usuario registra su número de teléfono, y de esta forma los centros de call center ya no pueden llamar a ese número.
The CAN-SPAM Act of 2003	Es la Ley en contra de contenido pornográfico y comercial no solicitado, donde obliga a los desarrolladores de tener un correo remitente que permita a las personas el poder oponerse a recibir esos correos. Y regulan las responsabilidades civiles y penales en caso de violar estas disposiciones.
Remsburg v. Docusearch[162]	La Suprema Corte de New Hampshire, determine que las compañías podían ser responsables pro como revelaban su información, ya que una empresa reveló información a un individuo que utiliza la información que le vendieron para tener información de una mujer y la mató. La empresa resultó responsable ya que no actuó con cuidado razonable al cuidar los datos de sus usuarios de terceros.

Siglo XXI: Una nueva década

Antes del 2016, con el fin de proteger los intereses de particulares, miles de empresas se adherían a los 7 principios internacionales del Safe Harbour, los cuales consistían en lo siguiente:

- **Informar**.- Las personas deben ser informadas de que sus datos están siendo recopilados y la manera en la que se utilizarán. Adicionalmente, se debe dar información relacionada a cómo ponerse en contacto con la organización con cualquier consulta o queja.
- **Elección** - Las personas deben tener la opción de optar por la colección y transferencia de sus datos a terceros.
- **Transferencias a terceros**- Las transferencias de datos a terceros sólo pueden efectuarse a otras organizaciones que sigan los principios adecuados de protección de datos.
- **Seguridad** - Deben realizarse esfuerzos razonables para evitar la pérdida de información recopilada.
- **Integridad de Datos** - Los datos deben ser relevantes y confiables para el propósito por el cual se recopilan
- **Acceso** - Las personas deben poder acceder a la información que se tiene sobre ellas, y podrán corregirlas o eliminarlas, si son inexactas.
- **Cumplimiento Forzoso** - Debe haber un medio eficaz de hacer cumplir estas reglas.

2017 en: http://www.law.nyu.edu/sites/default/files/ECM_PRO_062708.pdf
[162] http://caselaw.findlaw.com/nh-supreme-court/1132429.html

Sin embargo, debido a las revelaciones de Snowden, la Corte Europea de Justicia, determinó que los datos personales de los particulares de la unión europea no habían sido apropiadamente protegidos, y que fueron revelados a terceros sin consentimiento, por lo que determinaron que el Safe Harbour como sistema de auto cumplimiento ya no se consideraba válido para transferencia de información de datos personales de particulares de la unión europea.[163]

Es por ello que el 12 de julio de 2016, la Comisión Europea presentó al público el "Privacy Shield de la UE-EE. UU.", como sucesor del **"Safe Harbour Framework**", superará los altos requisitos que se deben cumplir al transferir datos personales de la Unión Europea a los Estados Unidos de América.[164]

De esta forma, en 2016, el Congreso de Estados Unidos promulgó la **Ley de Reclamación Judicial**[165], que otorga a los ciudadanos de ciertas naciones aliadas (en particular, los Estados miembros de la UE) el derecho de buscar reparación en las cortes estadounidenses por violaciones de privacidad.

Sin embargo ocurrió un problema este 2017, y esto debido a que en enero de 2017, **el nuevo presidente Donald Trump, emitió una orden ejecutiva, la cual incluye el siguiente párrafo:**

> *"Las entidades garantizarán que sus políticas de privacidad excluyan a las personas que no sean ciudadanos estadounidenses o residentes permanentes legales, de las protecciones de la Ley de Privacidad en lo que respecta a la información de identificación personal."*[166]

Definitivamente esta orden ejecutiva va en contra de los principios de la Privacy Shield y por lo tanto se presentarán varios problemas en un futuro para las empresas, ya que la orden ejecutiva

---

[163] Consultada en https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection el 20 de febrero de 2017.
[164] Consultado en http://www.lexology.com/library/detail.aspx?g=e02eccc0-9c26-4eb6-9293-00fb41272693 el 20 de febrero de 2017.
[165] Consultada en http://us.practicallaw.com/6-502-0467#a762707 el 20 de febrero de 2017.
[166] Consultada en http://www.michaelgeist.ca/2017/01/trumps-executive-order-eliminates-privacy-act-protections-for-foreigners/, el 20 de febrero de 2017. Texto original: *Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.*

les ordena a excluir a particulares que no sean residentes de los E.E.U.U.

ANEXO III. CATÁLOGO DE DELITOS SUCEPTIBLES DE COMETERSE A TRAVÉS DE MEDIOS ELECTRÓNICOS Y DELITOS CONSIDERADOS COMO INFORMÁTICOS, EN LA REPÚBLICA MEXICANA.

Entidad Federativa	Artículo	Delito	Modalidades
Baja California Sur	173 I.	Pornografía de menores de edad.	Por cualquier medio.
	241 X.	Fraude específico.	Acceso ilícito a programas informáticos.
	363	Usurpación de identidad.	Acceso ilícito a programas informáticos.
	356 IV, V.	Simulación de documentos equiparado.	Por medios electrónicos.
	357	Falsificación de contraseñas oficiales.	Falsificación de contraseñas
	359 II.	Falsificación de documentos.	Falsificación de medios de identificación electrónica
	362	Falsificación de documento tecnológico.	Por medios electrónicos.
	353	Violación de correspondencia.	Interceptar cualquier comunicación
	354	Violación de comunicación privada.	Cualquier medio de comunicación
	221	Revelación de secreto.	De cualquier forma
	222	Agravante revelación de secreto.	Secreto de carácter científico o tecnológico.
	382 I.	Sabotaje.	Vías de comunicación.
	363	Usurpación de identidad.	Por medios informáticos.
	331 II.	Uso indebido de los sistemas de emergencia y denuncia	Medios de comunicación, electrónicos, internet,
	364 I, III.	Usurpación equiparada.	Por medios informáticos.
Baja California	175	Revelación de secreto.	De cualquier forma
	175 Bis	Modificación o destrucción de información.	Sistemas o equipos informáticos.
	175 Ter	Acceso indebido a información.	Sistemas o equipos informáticos.
	175 Quinquies	Usurpación de identidad.	Cualquier medio.
	175 Quinquies I.	Usurpación equiparada.	Por medios informáticos.
	224 Bis	Agravante de extorsión.	Por medios electrónicos.
	259 3er párrafo	Falsificación de documentos.	Por dispositivos electrónicos.
	258	Falsificación de contraseñas.	Falsificación de contraseñas.
	257	Violación de correspondencia.	Interceptar cualquier comunicación
	262	Pornografía de menores de edad.	Por medios electrónicos.
		Turismo sexual.	Por cualquier medio.
	175 Sexties.	Delito contra la intimidad y la imagen.	Por cualquier medio.
	242 Bis.	Violencia Familiar.	Prohibición de ofender por medio electrónico.
	279 Bis.	Terrorismo.	Por cualquier medio.
	219 XI, XII	Fraude específico.	Por dispositivo o tarjeta plástica.
Chihuahua	226 Bis	Fraude equiparado.	Alteración informática.
	238	Destrucción, perdida de información.	Sistemas o equipos informáticos.
	327 Bis	Uso y acceso ilícito a los sistemas y equipos informáticos y de comunicación.	Sistemas o equipos informáticos.
	327 Ter		Sistemas o equipos informáticos.
	327 Quater.		Sistemas o equipos informáticos.
	327 Quiquies.		Sistemas o equipos informáticos.
	328	Falsificación de contraseñas oficiales.	Falsificación de contraseñas
	333	Falsificación de documento tecnológico.	Por cualquier medio.

	326	Violación de correspondencia.	Sistemas o equipos informáticos.
	327	Violación de comunicación privada.	Por cualquier medio.
	207	Revelación de secreto.	Secreto de carácter científico o tecnológico.
	284 Bis.	Delito contra la seguridad de la comunidad.	Canales de comunicación.
	325	Ataque a vías de comunicación.	Medios de comunicación.
	204 Bis.	Extorsión.	Por cualquier medio.
	183	Difusión de pornografía.	Por cualquier medio.
	181	Corrupción de menores.	Por cualquier medio.
	368	Defraudación fiscal.	Por cualquier medio.
Coahuila	281 Bis		Acceder a sistemas o equipos informáticos sin autorización
	281 Bis 1	Delitos contra la seguridad en los medios informáticos.	Accediendo con Información privilegiada.
	281 Bis 2		Acceder a sistemas o equipos informáticos del Estaado sin autorización
	281 Bis 3		Accediendo con Información privilegiada.
	294 II.	Falsificación de contraseñas oficiales.	Falsificaciones de contraseñas
	295 XI.	Falsificación de documentos.	Altere medios electrónicos.
	301	Pornografía infantil.	Por cualquier medio.
	372 II 4.	Secuestro calificado.	Por sistemas informáticos.
	272 Bis V	Falsificación de tarjetas de crédito.	Por dispositivo o tarjeta plástica.
	289	Violación de correspondencia.	Interceptar cualquier comunicación
	381	Revelación de secreto	De cualquier forma
	382	Violación de la privacidad.	Por medios técnicos.
	191	Conspiración política.	A través de medios electrónicos
	300	Distribución pornografía infantil.	Por cualquier medio.
	272 Bis V, VI	Agravante asociación delictuosa.	Posesión de dispositivos para falsificación de tarjetas.
	414 XI	Agravante robo.	Vales electrónicos, tarjeta plástica.
	307	Trata de personas.	Por cualquier medio.
	308	Lenocinio menores.	Por cualquier medio.
	298	Distribución pornografía infantil.	Por cualquier medio.
	376	Amenazas.	Por cualquier medio.
	399 Bis.	Acoso sexual.	Por medios informáticos.
Sonora	200	Falsificación de contraseñas.	Falsificación de contraseñas.
	200 Bis.	Clonación, falsificación y robo de información.	Por dispositivo electrónico.
	201	Falsificación de documentos.	A través de medios electrónicos
	152	Violación de correspondencia.	Interceptar cualquier comunicación
	176	Revelación de secreto.	De cualquier forma
	298 IV	Secuestro *	Revele datos o información.
	238	Amenazas.	Por cualquier medio.
	319	Fraude.	Por dispositivo electrónico, tarjeta plástica.
	241 Bis 1	Usurpación de identidad.	Tarjeta plástica, firma electrónica.
	308 X	Robo	Por dispositivo electrónico, tarjeta plástica.
	144 Bis.	Delincuencia organizada.	Organizarse por cualquier medio
	166	Exposición pública de pornografía.	Por cualquier medio
	169 Bis.	Difusión de pornografía.	Por cualquier medio.

	169 Bis 1.	Utilización de imagen y voz de menor de edad.	Por cualquier medio.
	128	Sedición.	Publicación de noticias.
	144 Bis 2.	Delitos contra el funcionamiento del sistema estatal de seguridad pública.	Intervenir cualquier medio de comunicación
	308 Bis III	Robo de vehículos.	Por cualquier medio.
Sinaloa	268	Falsificación de documentos.	Falsificar medios de identificación electrónica.
	271 Bis	Clonación, alteración de medios lectrónicos, uso indebido de información.	Altere medios de identificación electrónica. Tarjeta plástica.
	265	Violación de correspondencia.	Interceptar cualquier comunicación
	178	Revelación de secreto	De cualquier forma
	173 Bis	Cobranza ilegítima.	Por medios electrónicos.
	177 Bis	Usurpación de identidad.	Por cualquier medio.
	177 Bis A	Usurpación de identidad.	Por medios informáticos.
	216 IX	Fraude.	Por dispositivo electrónico.
	217	Delito informático.	intercepte bases de datos, sistemas informáticos.
	204 VIII	Agravante robo.	Por dispositivo electrónico, tarjeta plástica.
	274 Bis	Pornografía de menores de edad.	Por cualquier medio.
	274 Bis E	Turismo sexual.	Por cualquier medio.
	356 X, XI	Calumnia, propaganda electoral.	Por medios electrónicos.
	177	Violación de la privacidad.	Por cualquier medio.
Durango	400	Falsificación de tarjetas de crédito.	Dispositivos electrónicos, identificación electrónica, tarjeta plástica.
	401	Falsificación de contraseñas oficiales.	Falsificación de contraseñas.
	251	Violación de correspondencia.	Interceptar cualquier comunicación
	253	Omisión. Envío de mensaje.	Por empleado de estación inalambrica, telefónica.
	254	Violación de comunicación privada.	Cualquier medios de comunicación
	255	Delito contra la seguridad de la comunidad.	Posea dispositivos electrónicos que permitan interferir comunicaciones.
	256		Acceso ilícito a programas informáticos de empresa sin autorización
	257	Delitos contra la seguridad en los medios informáticos.	Acceso con información privilegiada
	258		Acceso ilícito a programas informáticos del Estado sin autorización
	259		Acceso con información privilegiada
	171	Violación de la privacidad.	
	172	Violación de la privacidad.	Por medios técnicos.
	240	Revelación de secreto	De cualquier forma
	168	Extorsión.	Por vía telefónica o medio de comunicación.
	228 XII	Delitos contra la seguridad pública y uso indebido de información.	Posea teléfonos móviles o medios de comunicación.
	249	Obstrucción de medio de comunicación.	Obstaculice vía de comunicación.
	320 IV	Acceso no autorizado a medios de información.	Radiofrecuencias, bases de datos, medios de comunicación.
	406	Uso indebido de llamadas telefónicas.	Por cualquier medio de comunicación.
	228 Bis	Obstrucción de seguridad pública.	Por cualquier medio.
	211 XXIII	Fraude.	Acceda a sistema informático.
	175 Bis	Usurpación de identidad.	Por cualquier medio.
	276	Pornografía de menores de edad.	Por cualquier medio.
	280	Difusión de pornografía.	Por cualquier medio.
	201 IV	Robo equiparado.	Datos de computadoras.

	287	Ultraje a la moral	Publique.
	174	Amenazas.	Por cualquier medio.
Nuevo León	242 Bis	Clonación de tarjetas.	Falsificar medios de identificación electrónica.
	243	Falsificación de contraseñas oficiales.	Falsificar contraseñas
	245	Falsificación de documentos.	De naturaleza electrónica
	178	Violación de correspondencia.	Interceptar cualquier comunicación
	223 Bis	Custodia de documentos equiparada.	Sustracción de datos de sistemas de cómputo.
	249	Falsedad de declaración.	Utilizando Internet.
	271 Bis 4	Agravante delitos sexuales.	Por medio de comunicación electrónica.
	385	Fraude.	Por medio de comunicación masivo.
	395	Agravante de chantaje.	Por medio de comunicación electrónica.
	444	Usurpación de identidad.	Por cualquier medio.
	408 Bis	Robo, fraude, abuso de confianza, usura, chantaje y administración fraudulenta.	Agravante. Por medio electrónico, tarjetas plásticas.
	201 Bis	Pornografía de menores de edad.	Por cualquier medio.
	201 Bis 2	Promoción de pornografía.	Por cualquier medio.
	365	Robo equiparado.	Por vía electrónica.
	427	Delitos por medios electrónicos.	Acceso indebido a sistema automatizado de datos.
	428		Supresión de datos de manera indebida
	429		Falsear de datos de manera indebida
	195	Ultraje a la moral *	Hacer circular públicamente.
	225 Bis 1	Acceso no autorizado a medios de información.	Sistema informático.
	225 Bis 2	Acceso indebido a medios de información.	Sistemas y equipos informáticos.
Tamaulipas	246	Falsificación de contraseñas oficiales.	Falsificar contraseñas
	175	Violación de correspondencia.	Interceptar cualquier comunicación
	205	Revelación de secreto.	Interceptar cualquier comunicación
	206		De cualquier forma
	207		Secreto de carácter industrial.
	207 Bis	Acceso ilícito a sistemas y equipos de informática.	Acceso sin autorización a sistemas y equipos informáticos de empresas.
	207 Ter		Acceso sin autorización a sistemas y equipos informáticos del Estado.
	207 Quater		Copie sin autorización sistemas y equipos informáticos del Estado.
	207 Quinquies		Modifique sin autorización sistemas y equipos informáticos del Estado
	207 Sexies		Copie indebidamente, aun estando autorizado contenido de sistemas y equipos infor
	194 Bis	Pornografía de menores de edad.	Por sistemas de cómputo o medios electrónicos.
	400 V	Robo de identidad.	Por cualquier medio.
	190	Ultraje a la moral *	Por cualquier medio.
	400 IV	Robo	Datos de computadoras.
	307	Amenazas.	Por cualquier medio.
Zacatecas	217	Falsificación de tarjetas de crédito.	Dispositivos electrónicos, identificación electrónica, tarjeta plástica.
	219	Falsificación de contraseñas oficiales.	Falsificar contraseñas
	220	Falsificación de contraseñas particulares.	Falsificar contraseñas
	227	Usurpación de identidad.	Por cualquier medio.
	257 Bis	Cobranza ilegítima.	Por medios electrónicos.

	257 Ter	Agravante cobranza ilegítima.	Por vía telefónica o medio de comunicación.
	151	Obstrucción de vías de comunicación.	Por cualquier medio.
	155	Violación de correspondencia.	Interceptar cualquier comunicación
	191	Revelación de secreto.	De cualquier forma
	192	Revelación de secreto industrial.	Secreto de carácter industrial.
	192 Bis	Delitos contra la seguridad en los medios informáticos y medios magnéticos.	Acceso ilítico a programas de cómputo.
	192 Ter		Alteración de sistemas o redes de cómputo.
	192 Quater		Acceso ilítico a programas de cómputo del Estado
	192 Quintus		Alteración de sistemas o redes de cómputo del Estado.
	229 IV	Acceso no autorizado a medios de información.	Bases de datos o cualquier medio de comunicación.
	257	Amenazas.	Por cualquier medio.
	340	Fraude.	Tarjeta plástica.
	321	Robo calificado.	Tarjeta plástica.
	181 Bis	Distribución pornografía infantil.	Por cualquier medio.
	183	Pornografía de menores de edad.	Por cualquier medio.
San Luis Potosí	251	Falsificación de documentos.	Por cualquier medio.
	256	Falsificación de contraseñas oficiales.	Falsificar contraseñas
	361	Violación de correspondencia.	Por empleado de empresa de comunicación.
	170	Uso ilícito de equipos de Radiocomunicación.	Radiocomunicación móvil.
	230	Extorsión agravante.	Por cualquier medio de comunicación.
	231	Extorsión cometida por empleados de empresas de comunicación.	Por empleado de empresa de comunicación.
	370 XI	Interferencia en el desarrollo del proceso electoral.	Por cualquier medio.
	212	Robo equiparado.	Datos de computadoras.
	277	Ultraje a a autoridad equiparado.	Por vía telefónica.
	168	Amenazas.	Por cualquier medio.
	178 Bis	Abuso sexual equiparado.	Por medios electrónicos.
Aguscalientes	160	Falsificación de contraseñas oficiales.	
	161	Falsificación de documentos.	Por dispositivo electrónico, tarjeta plástica.
	180	Violación de correspondencia.	Interceptar cualquier comunicación
	181	Acceso informático indebido.	Sistema operativo, computadora, archivo informático.
	179	Revelación de secreto.	Secreto de carácter industrial.
	149	Extorsión.	Por medio de comunicación electrónica.
	188 XVI G	Atentados al sistema de elección popular.	Por medio masivo de comunicación.
	189 VI, VIII	Atentados al sistema de elección popular. Equiparado.	Por medios de comunicación, internet.
	142 XI, XVI	Robo calificado.	Por sistemas informáticos.
	117	Pornografía de menores de edad.	Por cualquier medio.
	152 III	Daño de cosa ajena	Archivos, bases de datos.
	190 XIII, XIV, XV	Defraudación fiscal.	Alteración de sistemas informáticos.
	140 III	Robo.	Por servicio de internet.
	186	Sedición.	Por cualquier medio.
Guanajuato	232	Falsificación de contraseñas.	Falsificar contraseñas
	234 a	Falsificación y clonación de tarjetas.	Dispositivos electrónicos, tarjetas plásticas.
	231	Violación de correspondencia.	Contenida en equipos de cómputo.

	229	Revelación de secreto.	De cualquier forma
	245	Terrorismo.	Por cualquier medio.
	214 a	Usurpación de identidad.	Por cualquier medio.
	236	Pornografía de menores de edad.	Por cualquier medio.
	236 b	Distribución pornografía infantil.	Por cualquier medio.
	187 a	Acoso sexual.	Por cualquier medio. Pa
Jalisco	163	Falsificación de contraseñas oficiales.	Por cualquier medio.
	164	Falsificación de contraseñas particulares.	Falsificar contraseñas
	170 bis	Falsificación de medios electromagnéticos.	Acceda a sistema informático.
	143	Revelación de secreto.	De cualquier forma
	143 bis	Obtención ilícita de información electrónica.	Información contenida en equipos de informática.
	143 ter	Utilización ilícia de información confidencial.	Bases de datos, información confidencial.
	143 quater	Usurpación de identidad.	Por cualquier medio.
	125	Ataque a vías de comunicación.	Por cualquier medio.
	188	Amenazas.	Por cualquier medio.
Nayarit	240	Falsificación de contraseñas oficiales.	Falsificar contraseñas
	241	Falsificación de contraseñas particulares.	Falsificar contraseñas
	247 bis	Falsedad de informes dados a una autoridad.	Por cualquier medio de comunicación.
	173	Violación de correspondencia.	Interceptar cualquier comunicación
	208	Revelación de secreto.	De cualquier forma
	276	Amenazas.	Por cualquier medio.
	276 bis	Amenaza equiparada.	Por cualquier medio.
	291 b	Trata de personas.	Por cualquier medio.
	198	Ultraje a la moral *	Por cualquier medio.
Colima	253	Falsificación de conraseñas oficiales.	Falsificar contraseñas
	255	Falsificación de documentos.	Documento electrónico o firma electrónica.
	252	Violación de correspondenca.	Interceptar cualquier comunicación
	221	Revelación de secreto.	Secreto de carácter industrial.
	201	Fraude.	Disponer de mediosde disposición falsos
	290 III	Alteración de programas de cómputo (vehicular).	Equipos de cómputo.
	171	Pornografía de menores de edad.	Red, internet, dispositivos electrónicos, móviles, etc.
	172	Distribución pornografía infantil.	Por cualquier medio.
	174	Turismo sexual.	Por cualquier medio.
	204	Agravante de extorsión.	Vía telefónica, correo electrónico.
	249, 251	Ataque a vías de comunicación.	Por cualquier medio.
	259	Uso indebido de llamadas telefónicas.	Por cualquier medio.
	185	Robo calificado.	Información o documento electrónico.
	234	Ejercicio indebido de funciones.	Información o documento electrónico.
	170	Fabricación de pornografía.	Por medio de Internet o telefonía.
Michoacán	158	Pornografía de menores de edad.	Distribuirla a través de medios electrónicos
	296 fr IV, VI	Simulación de documentos	Sustraer información de la banda magnética de tarjetas
	289	Ataques a las vías de comunicación o	Cualquier medio de comunicación

		a los medios de transporte	
	301	Usurpación de identidad.	A través del mal uso de datos personales en bases de datos
	194	Ataques a intimidad	Divulgar por cualquier medio de comunicación
	217, 218 fr VI	Fraude.	Poner en circulación tarjetas falsas
	294	Violación de Correspondencia	Interceptar cualquier comunicación
	190	Revelación de Secreto	Revelarlo de cualquier forma
	314	Sabotaje de vías de comunicación del Estado	Cualquier medio de comunicación
	196	Ataques a la Propia Imagen	Divulgar por cualquier medio de comunicación
Hidalgo	203, 206 fr XIV	Robo	Agravante, si es a través de dispositivos electrónicos
	260	Violación de Correspondencia	Interceptar cualquier comunicación
	176	Revelación de Secreto	Revelarlo de cualquier forma
	262	Falsificación y uso indebido de sellos, marcas, llaves, contraseñas, u otros objetos	Falsificar contraseñas
	265 Bis	Falsificación de documentos (tarjetas, electromagnéticos, etc)	Alterar medios de identificación electrónica
	254	Ataques a las vías de comunicación o a los medios de transporte	Cualquier medio de comunicación
	213, 214 fr IX	Fraude	Uso de tarjetas de crédito falsas
	191	Difamación	Cualquier medio de comunicación
Querétaro	159 Ter	Acceso ilícito a sistemas y equipos de informática.	Acseso ilícito a sistemas y equipos de informática
	159 Quater	Acceso ilícito a sistemas y equipos de informática del Estado	Acceso ilícito a sistemas y equipos de informática
	193, 104 fr XVIII	Fraude	Uso de tarjetas de crédito falsas
	198 fr V	Extorsión	Agravante, si es a través de medios electrónicos
	232 Bis	Falsificación y Uso indebido de Documentos	Alterar medios de identificación electrónica
	223	Ataque a vías de comunicación.	Cualquier medio de comunicación
	229	Violación de Correspondencia	Interceptar cualquier comunicación
	159 Bis	Revelación de Secreto a través de medios electrónicos	A través de medios electrónicos
Estado de México	166 Bis fr V, VI, Ter	Delitos contra el funcionamiento del sistema estatal de seguridad pública.	Utilizar sistemas de comunicación electrónica prohibidos a sistemas de adaptación s
	167, 170	Falsificación de Documentos	Falsificar documentos electrónicos
	174 fr IV, V	Falsificación y Utilización Indebida de documentos de crédito	Falsificación de tarjetas de crédito
	204 fr III	Corrupción de menores. Pornografía en medios electrónicos	Divulgar a través de medios electrónicos
	266	Extorsión (agravante medios electrónicos)	A través de medios electrónicos
	268 Bis, Bis-1	Trata de personas.	Divulgar a través de medios electrónicos
	264	Usurpación de identidad.	A través del mal uso de datos personales en bases de datos
	197	Violación de Correspondencia	Interceptar cualquier comunicación
	116 Bis	Uso indebido de sistemas de emergencia	Cualquier medio de comunicación
	192	Ataque a vías de comunicación.	Cualquier medio de comunicación
	269 BIS	Acoso sexual.	Utilizar medios electrónicos
	305 FR x	Fraude	Poner en circulación tarjetas falsas
Ciudad de México	187	Pornografía Infantil.	Divulgar a través de medios electrónicos
	236	Extorsión	Agravante a través de medios electrónicos
	336 fr IV, V, VI	Falsificación de documentos de crédito	Alterar medios de identificación electrónica

	337	Falsificación de sellos, marcas, llaves cuños, troqueles, contraseñas, etc	Alterar Contraseñas
	333	Violación de correspondencia	Interceptar cualquier comunicación
	211 Bis	Usurpación de identidad.	A través de cualquier medio de comunicación
	213	Revelación de Secretos	Revelarlo de cualquier forma
	331	Ataques o daños a las vías de comunicación o a los medios de transporte	Cualquier medio de comunicación
	230, 231, fr XIV	Fraude	Cualquier medio de comunicación
	186	Turismo sexual.	Cualquier medio de comunicación
Tlaxcala	146 fr iv	Acceso ilícito a medios de comunicación de uso para la seguridad pública	Cualquier medio de comunicación
	308 fr II	Contra la seguridad de la comunidad, interferir comunicaciones	Cualquier medio de comunicación
	316	Contra la seguridad de medios informáticos (intervenir comunicaciones privadas)	Medios informáticos
	317	Intervenir comunciaciones de uan entidad pública	Cualquier medio de comunicación
	321, 324 Bis	Robo (Agravante cuando se robe a través de medios electrónicos)	Agravante, a través de medios electrónicos
	339	Fraude en medios electrónicos	A través de medios electrónicos
	331, 332 fr IV	Robo de Ganado, alterando dispositivos electrónicos	Alterando dispositivos electrónicos
	388	Ataque a vías de comunicación.	Cualquier medio de comunicación
	282	Usurpación de identidad.	Cualquier medio de comunicación
	392	Violación a la comunicación privada	Interceptar cualquier comunicación
	277	Revelación de Secretos	Revelarlo de cualquier forma
	134	Terrorismo.	Cualquier medio
	268,270	Extorsión a través de medios electrónicos	
	356	Contra la formación de menores de edad (pornografía)	Permitir acceso a visualizar contenido a través de cualquier medio
	398	Falsificación de Documentos electrónicos, tarjetas de crédito	A través de medios electrónicos
Morelos	148 Quáter	Delito informático.	Utilización dolosa de medios informáticos
	188,189, fr VIII, IX	Fraude	Utilizar dispositivos electrónicos falsos
	189 Bis	Suplantación de Identidad	Cualquier medio de comunicación
	220 Bis	Falsificación de sellos, marcas, llaves cuños, troqueles, contraseñas, etc	Falsificación de Contraseñas
	162 Bis	Turismo sexual.	Cualquier medio de comunicación
	267 Bis	Uso Indebido de Medios de Comunicación (avisos falsos de emergencia a través de medios de comunicación)	Cualquier medio de comunicación
	241	Violación de Correspondencia	Interceptar cualquier comunicación
	146	Extorsión	Cualquier medio de comunicación
	150	Violación de Intimidad Personal	Utilizar dispositivos electrónicos para ello
	211 ter	Corrupción de Menores pornografía	Permitir acceso a visualizar contenido a través de cualquier medio
Guerrero	173	Pornografía y Turismo Sexual de Menores de Edad	Divulgación a través de medios electrónicos
	344	Simulación de documentos	Falsificar tarjetas
	335	Ataques a vías de comunicación	Cualquier medio de comunicación
	237, 238 fr IX	Fraude	Acceder a programas informáticos del sistema financiero
	341	Violación de Correspondencia	Interceptar cualquier comunicación

	221	Revelación de Secreto	Revelarlo de cualquier forma
	342	Violación de comunicación privada.	Cualquier medio de comunicación
Puebla	220, 221, 222	Pornografía Infantil.	Almacenar/Distribuir por medio de comunicación
	245 Bis	Falsificación de documentos de crédito	Falsificar tarjetas
	248	Falsificación de sellos, marcas, llaves cuños, troqueles, contraseñas, etc	Falsificar Contraseñas
	195	Violación de correspondencia.	Interceptar cualquier comunicación
	230	Violación de Secretos	Revelarlo de cualquier forma
	475	Delito Informatico, hecho por un empleado de empresa, profesionista o funcionario	Acceso ilícito a sistemas de cómputo
	476	Delito Informático a empresas sin autorización	Acceso ilícito a sistemas de cómputo
	477	Delito Informático a alguna institución gubernamental sin autorización	Acceso ilícito a sistemas de cómputo
	478	Delito informático con autorización	Acceso ilícito a sistemas de cómputo
	402, 404 fr XXIV	Fraude	Usar tarjetas falsas
	186 Octies	Espionaje Contra Instituciones de Seguridad Pública	A través de cualquier medio
	188	Ataques a vías de comunicación	Cualquier medio de comunicación
	290 fr I	Amenazas	Cualquier medio de comunicación
	215	Ultrajes a la Moral Pública	Cualquier medio de comunicación
	292 Bis	Extorsión	Cualquier medio de comunicación
Veracruz	181	Delitos Informáticos	Acceso ilícito a sistemas de cómputo
	173 Bis	Engaño telefónico	A través de teléfono
	280 III.	Falsificación de títulos	Falsificar medios electrónicos
	177	Violación de Intimidad Personal	A través de cualquier medio
	178, 180	Revelación de Secretos	A través de cualquier medio de comunicación
	190 Quinquies V	Pederastia	Agravante. Por medios electrónicos
	190 Decies	Pornografía	Divulgar a través de medios electrónicos
	269	Delitos contra medios de Transporte y vías de comunicación	Cualquier medio de comunicación de una comunidad
	270	Delitos contra medios de Transporte y vías de comunicación	Dañar cualquier medio de comunicación
	272	Delitos contra medios de Transporte y vías de comunicación	Quitar cualquier medio de comunicación
	273	Violación de Correspondencia	Interceptar cualquier comunicación
	216, 217	Fraude	Utilizar tarjetas falsas
	278	Falsificación de sellos, marcas, llaves cuños, troqueles, contraseñas, etc	Falsificación de Contraseñas
	311	Terrorismo	Por cualquier medio
	190 sexies	Corrupción de Menores	Facilitar contenido pornográfico a través de cualquier medio
	264 quinquies.	Crueldad de Animales	Agravante. Por medios electrónicos
	178	Revelación de Secreto	Revelarlo de cualquier forma
Oaxaca	165 Ter III	Divulgación de Datos	Divulgar datos dentro de sistemas informáticos
	195 fr I	Pornografía Infantil.	Divulgar a través de medios electrónicos
	241	Acoso Sexual	A través de medios electrónicos
	264 I	Amenazas	Cualquier medio de comunicación
	348 Bis	Secuestro Expres	A través de medios electrónicos
	383 IV	Extorsión	Agravante. Por medios electrónicos

	138 I	Rebelión y Espionaje	Interferir medios de comunicación
	169 VI	Interrupción de Vías de Comunicación	Cualquier medio de comunicación
	174 I	Violación de Correspondencia	Interceptar cualquier comunicación
Tabasco	326 bis	Acceso sin autorización de medios informáticos	Acceso ilícito a sistemas de cómputo
	326 Bis 1	Daño informático.	Alteración de datos en medios informáticos
	326 bis 2	Falsificación informática.	Falsificación de documentos en medios informáticos
	338 bis	Contra la seguridad y orden en los centros de detención.	Utilizar sistemas de comunicación electrónica prohibidos a sistemas de adaptación
	315	Violación de correspondencia.	Interceptar cualquier comunicación
	164	Revelación de secreto.	Revelarlo de cualquier forma
	307 I, III	Interrupción del servicio público de comunicación.	Cualquier medio de comunicación
	309	Interrupción del servicio público de comunicación.	Cualquier medio de comunicación
	312 Bis	Uso indebido de los servicios de emergencia.	Cualquier medio de comunicación
	316	Violación de la comunicación privada.	Cualquier medio de comunicación
	363 IV	Sabotaje.	Alterar cualquier medio de comunicación del Estado.
	163 III.	Violación de la intimidad personal.	Utilizar dispositivos electrónicos para ello
Chiapas	228 Bis	Engaño.	A través de medios electrónicos
	301 VI	Extorsión	Agravante. Por medios electrónicos
	333	Pornografía infantil.	A través de medios electrónicos
	405	Falsificación de tarjetas.	Falsificación de tarjetas.
	347	Rebelión.	Alterar cualquier medio de comunicación del Estado.
	353 III	Motín	Obstruir cualquier medio de comunicación
	382 I, III	Ataques a vías de comunicación.	Cualquier medio de comunicación
	386	Violación de correspondencia.	Interceptar cualquier comunicación
	390	Intervención ilegal de comunicación privada.	Cualquier medio de comunicación
	435	Revelación de secretos.	Revelarlo de cualquier forma
	302 XXIV	Fraude	A través de sistemas informáticos
Campeche	172	Amenazas	Agravante. Por medios electrónicos
	175 III	Violación a la intimidad.	A través de medios electrónicos
	182	Revelación de secretos.	Cualquier medio de comunicación
	209, 210 fr III	Extorsión.	A través de medios electrónicos
	229	Delitos contra el servicio público de comunicación.	Dañar cualquier medio de comunicación
	230	Delitos contra el servicio público de comunicación.	Interrumpir cualquier medio comunicación
	235	Violación de correspondencia.	Interceptar cualquier comunicación
	249	Calumnia	Agravante. Por medios electrónicos
	255	Corrupción de menores.	Facilitar contenido pornográfico a través de cualquier medio
	260 I.	Pornografía de menores.	A través de medios electrónicos
	373	Rebelión.	Alterar cualquier medio de comunicación del Estado.
	385	Delitos contra animales.	Difundir maltrato a través de medios electrónicos
	207 XII	Fraude.	Uso de tarjetas falsas
	237	Falsificación de contraseñas oficiales.	Falsificación de contraseñas

	240 IX	Falsificación de documentos.	Falsificación de medios electrónicos
Yucatán	165 Sexies I, II	Delitos contra el funcionamiento del sistema estatal de seguridad pública.	Ingresar ilícitamente a sistemas informáticos del Estado.
	211	Pornografía de menores.	Divulgar a través de medios electrónicos
	243 Bis 2 I, III	Delito contra la intimidad personal.	Divulgar a través de medios electrónicos
	284 Bis	Falsificación de documentos.	Falsificar tarjetas, medios de identificación electrónica, etc.
	304	Delitos contra el honor.	A través de medios electrónicos
	140 I	Rebelión.	Alterar cualquier medio de comunicación del Estado.
	167	Delitos contra la seguridad de las vías de comunicación.	Dañar Cualquier medio de comunicación
	168	Delitos contra la seguridad de las vías de comunicación.	Destruir Cualquier medio de comunicación
	174	Violación de correspondencia.	Interceptar cualquier comunicación
	207	Ultrajes a la moral.	Divulgar por cualquier medio
	279	Falsificación de contraseñas oficiales.	Falsificar contraseñas
Quintana Roo	156	Extorsión	Agravante. Por medios electrónicos
	189, 189 Bis	Falsificación de documentos.	Agravante. Por medios electrónicos
	192 Bis II, III	Pornografía infantil.	Divulgar por cualquier medio
	195 sexties.	Usurpación de identidad.	Por cualquier medio
	195 septies II , IV	Usurpación de identidad equiparada.	Por medios electrónicos
	182	Ataques a vías de comunicación.	Cualquier medio de comunicación
	187	Violación de correspondencia.	Interceptar cualquier comunicación
	153 XV	Fraude.	Utilizar tarjetas falsas
	126	Revelación de secretos.	Revelarlo de cualquier forma

SYNTHÈSE DE LA THÈSE EN FRANÇAIS

CHAPITRE I

LE CONCEPT D'IDENTITÉ NUMÉRIQUE

1.1 CONCEPT D'IDENTITÉ HOLISTIQUE

Tout au long de l'histoire, l'identité a obéit à une tendance : identifier, dans tous les cas, signifie singulariser.

Au Moyen Age, l'identité devait être lisible et visible, il y avait donc un lien étroit entre l'identité et l'habillement, afin de classer les habitants et donc de leur accorder le traitement approprié, en termes de prérogatives ou de restrictions, en fonction de leur rôle dans la société.

L'identification écrite est imposée depuis le quatorzième siècle, toujours afin de délimiter l'identité individuelle par les autorités.

La systématisation de l'identification répond successivement à la nécessité statistique qui impose une connaissance précise de la population, à la conformation et à la mobilisation de l'armée et à la création de plans de développement social.

De nos jours, il y existe une ambition croissante de décrire l'individu à un tel niveau de détail que ses caractéristiques physiques et ses signes particuliers servent à leur identification plus précise. Avec l'aide de certaines sciences auxiliaires, telles que l'anthropométrie et la biométrie, un individu peut aujourd'hui être identifié presque infailliblement.

Le concept d'individu a généralement des significations différentes, biologiques, sociologiques et anthropologiques. Par exemple, celle que j'utiliserai tout au long de cette étude et qui est définie par l'Académie royale espagnole : dans son sens familier "Personne, en faisant abstraction des autres ". Précisément parce que l'idée d'identité que je veux explorer, est celle qui nous donne des éléments de différenciation du commun des mortels, qui nous sort de l'anonymat, qui nous rend spéciaux et uniques en termes d'appartenance à une société.

Cet ensemble de caractéristiques d'un individu, par rapport à un groupe d'individus qui l'entoure, s'appelle identité.

Du latin identitas, l'identité est l'ensemble des caractéristiques d'un individu ou d'une communauté. Ces traits caractérisent le sujet ou la communauté comparés aux autres.

L'identité est aussi la conscience qu'une personne a de soi et qui la distingue des autres. Bien que de nombreux traits qui forment l'identité soient héréditaires ou innés, l'environnement exerce une grande influence sur la génération de la spécificité de chaque sujet.

Du Dictionnaire de l'Académie royale de la langue espagnole, nous pouvons extraire la définition suivante :

Identité
(D'après lat.identĭtas, -ātis).
1. f. Qualité d'identique.
2. f. Ensemble de caractéristiques d'un individu ou d'une communauté qui les caractérisent face aux autres.
3. f. Conscience qu'une personne doit être elle-même et différente des autres.
4. f. Fait d'être quelqu'un ou quelque chose, le même qui se suppose où se recherche.
5. f. Mat. L'égalité algébrique toujours vérifiée, quelle que soit la valeur de ses variables.

En analysant les différentes significations de la définition proposée, nous pouvons dire ce qui suit :

1. La qualité d´identique nous dit que lorsque l'on compare quelque chose avec sa similitude, il s'avère être le même, c'est-à-dire qu'il nous parle des caractéristiques de quelque chose ou de quelqu'un qui coïncide avec un autre de sa même classe ou espèce.

2. Quand on parle d'individus ou de collectivités, naît le besoin de trouver leurs propres caractéristiques, celles qui les différencient les uns des autres.

3. L'individu, tout au long de sa vie, crée des traits qui lui sont propres pour se

distinguer des autres. En effet, la recherche de son identité devient, dans de nombreux cas, une lutte continue et nécessaire, puisque s´il n'y avait pas d'autres individu, il ne serait pas possible de discriminer les autres.

4. Le mot "identité" dans la langue des chercheurs, s´utilise lorsqu'il y a quelque chose ou quelqu'un dont l'identité ou la personnalité devrait être accréditée.

5. Même dans le langage mathématique, nous reprenons les concepts de comparaison et d'égalité.

1.2 IDENTITÉ EN TANT QUE FIN PRIMAIRE DE L'INDIVIDU.

Comme nous l'avons mentionné précédemment, l'identité doit être entendue au-delà d'un simple contexte sémantique, elle devient une fin en soi, la compréhension de l'individu comme élément unique, précieux, digne et primordial de la société, c´est alors que l´on donne enfin un sens à sa vie. Par conséquent, le but premier de l'être humain devrait être de trouver sa place dans le monde, de visualiser et d'assumer dans son ensemble d´être un être composé d'éléments tangibles et intangibles, tels que sa structure la plus fondamentale, c'est-à-dire son anatomie, mais aussi ses éléments de nature philosophique, psychologique et, en général, de personnalité. Dans leur ensemble, ces éléments constituent ce que nous considérons « Un individu ».

Carl Jung, membre du courant de psychologie analytique, supposait que le but suprême de la vie est l'individualisation. Les expériences de l'enfance et celles de la maturité, les espoirs du futur font que l'individu est ce qu'il est. En parlant de lui-même, il disait : « Ma vie est un cas de réalisation de soi de l'inconscient. Tout y cherche sa manifestation extérieure, et la personnalité évolue aussi pour sortir de ses états inconscients. "

Pour lui, l'individualisation est un état de santé psychologique qui découle de l'intégration de tous les aspects, conscients et inconscients, de la personnalité. Bref, l'individualisation implique de devenir un individu, de réaliser ses capacités et de se développer soi-même. La tendance à l'individualisation est innée et inévitable, mais les forces environnementales, telles que les opportunités économiques et éducatives et la nature de la relation parent-enfant, la conduisent ou l'entravent.

Pour atteindre l'individualisation, les gens doivent abandonner les comportements et les valeurs qui les ont dirigés dans la première moitié de leurs vies et faire face à l'inconscient, amenant à être conscient et en acceptant ce qu'il leur demande de faire. Ils doivent écouter ce que leurs rêves disent et suivre leurs fantasmes, en exerçant une imagination créative, en écrivant, en peignant ou en utilisant un autre type d'expression. Alors seulement, le soi se révélera.

Bien sûr qu´il ne faisait pas l´éloge de se laisser dominer par l'inconscient, mais plutôt d´etre capable de s'équilibrer avec la force consciente pour devenir un individu émotionnellement mature ; à ce que personnellement j'appellerais se connaitre et se gouverner.

Plus tard, cette théorie soutiendra l'hypothèse selon laquelle de nombreux sujets qui ont réprimé leurs instincts les plus primitifs et qui ont une personnalité introvertie, laissent souvent sortir ce groupe d'éléments de la personnalité réelle à travers leurs « avatars » ou personnages des réseaux sociaux.

À cet égard, Jean-Claude Filloux, dans son livre La personnalité, suppose que la psychologie a comme objectif essentiel, la connaissance de l'individu comme entité particulière « nous ne sommes jamais devant l'homme en général, mais toujours devant un homme particulier, un individu qui est souvent une énigme, un problème et nous savons que la solution ne peut pas être trouvé sauf en lui-même. La caractéristique la plus essentielle de l'homme est son individualité ». "

Filloux met en évidence un élément qui coïncide parfaitement avec ma position sur le sujet : l'homme, par son individualité, se manifeste et se comporte comme nul autre, puisque ce comportement n'appartient qu'à lui. Bien qu'il soit vrai que l'homme est une entité sociale et en tant que tel, imprégné des influences exercées par la société dans sa vie, il conserve malgré tout ses propres éléments qui servent à le distinguer comme une entité particulière et unique.

Je base ma position précédente, en ce qui concerne la dignité de l'homme, en coïncidant avec ce que le Dr Carlos Llano Cifuentes plaide dans son travail "Voyage au centre de l'homme ». L'être humain par le simple fait d'exister, est une entité dotée de dignité, de valeur en soi, une valeur qui parvient à doter tous les faits qui émanent de lui d´une valeur spécifique. Leurs actes sont précieux par leur simple origine, c'est-à-dire qu'ils proviennent de l'être humain et, par conséquent, d'un être digne. "Chaque individu, chacun de nous, bien qu'il se connaisse limité par sa naissance et sa mort et par toutes les circonstances qui le contraignent et l'appauvrissent, a une valeur infinie".

Mais, sans aucun doute, l'essence de la pensée de l'auteur que je veux souligner comme fondement de ma position sur la valeur de chacun de nous en tant qu'individu, c'est que les gens ne sont pas interchangeables parce qu'ils sont en soi un univers complet.

1.3 L'IDENTITÉ EN TANT QUE VALEUR JURIDIQUE

Le droit à l'identité est l'un des droits fondamentaux de tout être humain, et il est nécessaire pour pouvoir bénéficier des autres droits fondamentaux.

Depuis notre naissance, nous avons nos propres droits d'identité, par exemple, le droit d'avoir un prénom et un nom de famille. L'organisation internationale à but non lucratif, Humanium, souligne les droits suivants de l'enfant en matière d'identité :

"Le droit de l'enfant à l'identité : Dès la naissance, toute personne a le droit d'obtenir une identité. L'identité comprend le nom, le prénom, la date de naissance, le sexe et la nationalité. C'est la preuve de l'existence d'une personne en tant que membre d'une société, en tant qu'individu faisant partie d'un tout ; c'est ce qui le caractérise et la différence des autres.

Tous les enfants ont le droit d'avoir une identité officielle, c'est-à-dire d'avoir un nom, un nom de famille, une nationalité et de connaître l'identité de leurs parents.

Droit à un nom et à un prénom : Dès la naissance, l'enfant a le droit d'avoir un nom et un nom de famille. Tous les enfants doivent être enregistrés immédiatement après leur naissance, puisque les parents ont l'obligation d'informer du nom, prénom et de la date de naissance du nouveau-né.

Cette action implique la reconnaissance immédiate par l'Etat de l'existence de l'enfant et la formalisation de sa naissance devant la loi. De plus, son enregistrement permettra à l'enfant de préserver ses origines, c'est-à-dire les liens de parenté qui le lient à ses parents biologiques.

Droit à la nationalité : Depuis sa naissance, l'enfant a le droit d'acquérir une nationalité. "

Les attributs de la personnalité, en droit, sont les propriétés ou les caractéristiques identitaires des individus ou des entités juridiques en tant que détenteurs de droits.

Jeremy Antippas, diplômé de l'Université Panthéon-Assas, explique dans sa thèse de doctorat, concernant les droits de la personnalité, qu '"ils peuvent être définis comme les droits qui assurent à l'individu la réserve des attributs de sa personne, soit garantissant son intégrité morale: comme le droit au secret de la vie privée, le droit à l'image, la voix et le nom de famille, le droit au respect de l'honneur et la présomption d'innocence et la dignité de la personne humaine, en bref, le droit moral, par les auteurs, artistes, interprètes d'œuvres intellectuelles qui constituent l'expression de leur personnalité. La théorie générale des droits de la personnalité en France est le résultat d'un travail acharné de la doctrine et de la jurisprudence privée pendant environ un siècle.

Elle est complétée par l'étude d'une multiplicité de domaines du droit, non seulement le droit civil mais aussi le droit pénal, la propriété intellectuelle, etc.

Il convient de noter que l'accent qu'il met sur le postulat selon lequel les droits de la personnalité sont traditionnellement nés de la doctrine du droit civil ont progressivement migré vers le droit administratif. Certes, au Mexique, il en est de même, si l'on tient compte du fait que l'autorité fédérale de protection des données personnelles des citoyens mexicains, l'Institut fédéral d'accès à l'information et de protection des données (IFAI), est récemment devenue un organisme autonome changeant son nom en INAI, il est de nature administrative, tout comme l'autorité de contrepartie en France, la Commission Nationale de l'Informatique et des Libertés (CNIL).

A l'origine, pour définir la personnalité et ses attributs, nous nous référions aux concepts de la doctrine civiliste ; cependant, de nos jours, la tendance est de multiplier et de diversifier les domaines du droit qui traitent du problème de la définition, de la reconnaissance, de la protection, de l'authentification et de la sauvegarde de l'identité de la personne. Des exemples de cela sont les contributions faites par Alfredo Reyes Krafft, Hans Valadez Martínez et Guillermo Tenorio Cueto, dans le livre coordonné par ce dernier, intitulé Los Datos Personales en México. Perspectives et défis de sa gestion en possession des individus.

En France, le droit à l'identité, entendu comme l'ensemble des caractéristiques qui nous distinguent d'un autre individu, est principalement reflété dans le Code civil, hérité de la Déclaration des droits de l'homme et du citoyen de 1789.

L'article 9 du Code civil français consacre le droit au respect de la vie privée et

donne aux autorités judiciaires toute autorité pour prendre les mesures nécessaires à sa sauvegarde. Par conséquent, les droits de la personnalité et de l'essence prétorienne sont définis comme des attributs dont tous les êtres susceptibles de droits et d'obligations sont dotés ; sous-entendu leur droit à la reconnaissance et au respect de leur personnalité. C'est pourquoi, diverses lois à travers le monde traitent les crimes contre la personnalité et l'image publique. Les principaux acteurs contre ces activités, étant donné qu'ils sont les plus touchés, sont les personnes célèbres, de la vie politique ou artistique car un acte illicite qui porte atteinte à sa réputation a un impact massif beaucoup plus important que pour tout autre individu, même si ceux-ci ne sont pas moins importants.

La loi du 17 juillet 1970 consacre le travail jurisprudentiel français, sans le laisser inerte, pour que les tribunaux disposent d'une base juridique solide, riche de nouveaux critères permettant d'améliorer la protection efficace de la vie privée. L'évolution jurisprudentielle est telle que même les criminels ont un droit à l'oubli qui permet leur réintégration sociale.

L'intérêt social consacré dans le droit à l'information est limité à tout moment par le droit à la vie privée et le respect de la personnalité. On recherche une interaction saine entre les deux à tout moment et que leur application ne soit envahissante ni pour l'un ni pour l'autre. Cela dit, en cas de litige, les tribunaux français ont choisi de faire prévaloir les droits personnels.

En matière de droit d'auteur, c'est une atteinte au commerce d'utiliser l'image d'une personne sans son autorisation ou celle de ses ayants droit ; Grâce à l'analyse de l'article 73 du règlement de la loi fédérale sur le droit d'auteur, Manuel Magaña déduit que l'image d'une personne comporte trois éléments de base :

1) "Le visage ;

2) l'expression corporelle ; et

3) Traits ou caractéristiques générales, même si celles-ci ont été modifiées ou déformées, ou si le nom de la personne a été remplacé. Si l'image fait référence à une personne, vous devez avoir son autorisation. "

L'identité personnelle est une notion typique des mentalités qui respectent l'individualité humaine - des opinions intellectuelles qui évitent d'utiliser les collectivités comme axe de la

pensée.

En fin de compte, quand nous n'avons rien, quand nous nous regardons dans le miroir nu et dans la solitude, nous n'avons que ce que nous sommes réellement, notre identité. Comme l'a exprimé Viktor Frankl dans son livre "L'homme en quête de sens", l'existence nue, "Alors que nous attendions la douche, notre nudité nous a été clairement expliquée, dans son sens littéral : nous n'étions qu'un corps. Rien de plus. Nous possédions seulement l'existence nue. "

1.4 IDENTITÉ NUMÉRIQUE

Au-delà des fondements de la génétique, de la biologie, de la psychologie, de la sociologie et en général de tous les éléments culturels qui composent l'identité humaine, on peut aujourd'hui ajouter un nouveau concept : l'identité numérique.

Il est important de souligner que le concept d'identité numérique n'est pas présent exclusivement sur Internet, judicieusement et parfaitement décrit comme « un canal global de télécommunications informatiques intégrées par de nombreux canaux qui, à leur tour, sont interconnectés les uns avec les autres », c´est alors qu´il nous tient connectés et en communication, très exposés. Mais ce concept est aussi dans notre vie quotidienne. Par exemple, dans l'entreprise, sur nos comptes bancaires, à la sécurité sociale et en général dans presque tous les domaines de notre vie.

Cette identité numérique est composée de différents identifiants généralement mal gérés, et dans le pire des cas, nous n'en avons même pas conscience.

Aujourd'hui, nous sommes immergés dans la société de l'information. Notre identité numérique devient non seulement notre clé pour y accéder, mais la lettre de présentation avec laquelle nous joueons et nous nous y développons. Comme expliqué tout au long de ce travail, l'identité numérique va au-delà d'une simple question d'identification. En effet, précisément à cause la complexité de l'identité numérique, il est parfois difficile d'identifier le sujet qui se cache derrière un certain niveau d'anonymat.

L'importance de cette étude est d'approfondir à travers une réflexion juridique méthodique, le problème de la gestion et de la protection de notre identité numérique qui se compose de différents aspects, à la fois techniques, juridiques, éthiques, économiques et même psychosociaux.

1.4.1 CONCEPT ET ÉLÉMENTS DE NOTRE IDENTITÉ NUMÉRIQUE.

Je vais donc présenter le concept d'identité numérique que nous avons élaboré et sur lequel nous développons cette étude, puisque nous y ferons référence en permanence.

L'identité numérique est l'ensemble des éléments d'identification et de personnalisation de l'individu qui lui permette de naviguer dans le milieu électronique sans notion de temps ou d´espace.

L'identité numérique peut également être définie comme quelque chose de plus profond et qui se construit constamment. C´est à dire qu´elle se compose de « traces » que nous laissons consciemment ou inconsciemment dans le monde numérique, principalement dans nos navigateurs. Par exemple, notre historique de recherches, les vidéos que nous avons consultés, les cookies qui restent sur notre ordinateur, les « j'aime » sur Facebook, définissent peu à peu qui nous sommes ou notre identité numérique.

À ce stade, on peut se demander valablement, si cette identité n'est alors rien de plus qu'une extension de notre identité quotidienne du monde tangible, puisque de nombreuses études ont montré que tout ce qui arrive à notre identité numérique ou virtuelle, a un impact sur notre environnement physique. Les cas où les personnes ont été exposées au harcèlement sexuel par la réalité virtuelle ont reportés des effets psychologiques post-traumatiques.

Un aspect très important des effets réels, qu´ils soient physiques, psychologiques ou émotionnels, engendrés par l'agression de notre identité numérique a été analysé dans une étude de l'Université de Stanford, menée par Cynthia McKelvey. Elle a démontré que les simples connotations sexuelles des avatars féminins de certains jeux vidéo, par leurs vêtements et apparence, ont un effet négatif sur la société en représentant les femmes comme une « chose » et les convertissant en un simple objet, peuvent se convertir en une fausse justification de violation pour les hommes.

Comme antérieurement expliqué et vue l'importance de comprendre la portée de l'information qui fait notre identité numérique, nous la décrirons. Cet ensemble d'éléments d'identification peut varier d'un pseudonyme ou nom d'utilisateur (qui ne coïncide pas toujours avec le réel), à des éléments qui ne sont pas spécifiques à l'individu, mais qui peuvent être utilisés à une heure et un endroit précis pour s´ identifier, comme l'adresse IP d'un ordinateur. C´est à dire

que pour reconnaître tous ces éléments « identifiants » qui pourraient éventuellement faire partie de l'identité numérique d'une personne, on devra d´abord les reconnaître en leur qualité de données personnelles pour pouvoir alors les protégées correctement.

Un système d'identité, qu´il soit réel ou électronique, se base sur l'ensemble des « identifiants » dans le monde réel, par exemple, le nom, prénom, date et lieu de naissance, RFC, numéro de sécurité sociale, etc., et dans le monde virtuel, où il existe d'autres types d'identifiants tels que les pseudonymes, courriels, avatars, etc.

Il existe une catégorie d'identificateurs accordés par l'État comme c´est le cas de CURP au Mexique. Il s´agit d´un code de registre unique de la population émis par l´organisme de Registre national de la population qui sert d'identifiant unique visant à identifier chacun des citoyens du Mexique. De même sont reconnus comme Documents officiels: la carte d'électeur ou l'acronyme INE Institut national électoral, qui contient plusieurs données importantes telles que le nom et l'adresse du propriétaire, sa photographie et sa signature; le Passeport, délivré par le ministère des Affaires étrangères, qui contient le nom complet, sa photographie et sa signature ; le certificat professionnel avec sa photographie et sa signature, délivré par le Ministère de l'Éducation Publique ; la Carte de Service Militaire National, délivrée par le Secrétaire de la Défense Nationale (pour ceux qui la détiennent); et enfin, toute identification officielle valide avec photographie et signature, émises par le gouvernement fédéral, étatique ou municipal de Mexico.

Aux États-Unis, par exemple, il n'y a pas d'identification nationale officielle. En vertu de la Real ID Act approuvée par le Congrès américain en 2005, au lieu de nommer un document d´identification, il a été établi des paramètres minimaux de données personnelles que doit contenir un document identificateur pour être considéré comme valide.

Et enfin, dans le cas de la France, il existe la Carte Nationale d'Identité, qui sert de pièce d'identité nationale accordée à tous les français de tous les âges par les textes réglementaires 55 du décret nº -1397 du 22 octobre 1955 relatif à la carte d'identité, n ° 55-1397 Décret du 22 octobre 1955 relatif à la carte d'identité et du 1er mars Circulaire 2010 relatif à la simplification de la Délivrance des cartes Nationales d'Identité et des passeports. Cette identification est valable pour 15 ans renouvelables, elle contient des éléments de base pour l'accréditation de l'identité sur le territoire français, comme le prénom (s), nom (s), date et lieu de naissance, la taille, le sexe, le domicile ou la résidence de la partie intéressée et même la signature et la photographie de celle-ci.

Il existe également d'autres identifiants qui sont utilisés pour traiter certains services publics comme, au Mexique, la signature électronique avancée que la SAT récemment renommée « e. firma ». Cet e. firma est un fichier numérique qui identifie les personnes physiques et morales et permet d'effectuer des procédures via Internet dans le SAT et dans d'autres dépendances du Gouvernement de la République.

Il s'agit d'un certificat numérique qui contient une clé publique et une clé privée, utilisant une cryptographie asymétrique. Il convient de noter que l'une de ses principales caractéristiques est l'attribution unique, c'est-à-dire qu'elle identifie de façon unique son utilisateur. Pour l´avoir, une série de documents qui ont permis d'accréditer la personnalité du propriétaire par l'agent de certification sont necessaires en plus de la Signature électronique avancée du demandeur. Ceci a révolutionné la vie des Mexicains ou étrangers résidant au Mexique, permettant non seulement d'effectuer des transactions par Internet plus simples et la signature de contrats à distance facilités mais aussi de réduire de manière significative le vol d'identité.

La biométrie est un autre élément important de notre identité car elle prend en compte les éléments biologiques de l'être humain, comme une partie du corps que l´individu ne peut pas modifier. Différentes méthodes d'identification biométriques sont utilisées actuellement, la plus populaire étant l'empreinte digitale, mais ces derniers temps la reconnaissance vocale et faciale sont devenues courantes car elle présente diverses options : l'iris, le rythme et la pression du pouls, l'odeur corporelle, la démarche, etc.

Dans la pratique, l'utilisation de la technologie biométrique pour l'identification des personnes a autant de partisans que d´opposants. Elle est plus fréquemment utiliser pour le contrôle d'accès, même si dernièrement elle sert également à sécuriser les transactions bancaires ou économiques, comme par exemple Face ID d'Apple, qui permet d'effectuer des achats avec un portefeuille Apple Pay ou avec d'autres fournisseurs tels que PayPal.

Avec l'augmentation alarmante des cas d'usurpation d´identité à travers le monde, l'identification biométrique devient une alternative intéressante car il est de plus en plus difficile de vérifier, par des documents ou même face à face, l'identité réelle d'un individu. La technologie est une nouvelle alternative pour avoir un support de confiance ; cependant, toute technologie est susceptible d'être violée ; et c´est cet argument que mettent en avant les opposants à l'utilisation de la technologie biométrique refusant sa démocratisation, même si elle était annexée aux cartes

d´identité nationales ou aux passeports nationaux.

Au Mexique, depuis 2016, le Système d'épargne retraite (SAR) a mis en place l'utilisation de la biométrie afin que les travailleurs puissent réaliser des opérations sur leurs comptes AFORE[167]. L'intégration de la biométrie dans le système de retraite apportera de nombreux avantages aux travailleurs, dont :

- Sécurité dans toutes les procédures SAR. Il est possible de confirmer à 100% l'identité des travailleurs : Cela permettra également d'éviter les comptes multiples ou l´attaque de comptes.
- Rapidité lors de nouvelles démarches administratives, Aucune autre documentation ne sera requise, ce qui facilitera la gestion des formulaires et des demandes
- Diminution des coûts administratifs pour les travailleurs. En remplaçant les papiers par des formats électroniques, on estime que les frais de gestion diminueront de 50 à 70% (on prend en compte les articles de papeterie, les photocopies, la numérisation, les envois et les colis, les impressions et les captures).
- Meilleur contrôle des procédures, Ce qui empêchera toute pratique inappropriée.[168]

Il existe d'autres types d'identifiants, strictement « virtuels », qui ont été le plus souvent choisis par les personnes eux-mêmes : par exemple à l'époque du boom des courriers électroniques, il y a plus de vingt ans, lorsque les services tels que Yahoo!, Hotmail, Gmail, etc., se sont popularisés, il était beaucoup plus facile d'avoir un email avec notre nom ou un "alias" de notre prédilection. De nos jours, avec plus de millions de comptes email dans le monde, les adresses disponibles sont très limitées, sans compter le fait qu'elles sont maintenant constituées de divers caractères alphanumériques et spéciaux.

Nous avons aussi des comptes de réseaux sociaux, tels que Twitter, Snapchat, Pinterest, Instagram, Tinder, etc., qui nous permettent de créer des comptes avec nos données réelles, ou d'utiliser des alias pour conserver un certain anonymat.

[167] Gestionnaires de Fonds de retraite
[168] L´introduction du Biométrique dans la gestión des comptes AFORE permet au Sisteme des Retraites d´etre à la pointe du progres tecnologique du sisteme financier. Voir: https://www.gob.mx/consar/prensa/la-introduccion-de-biometricos-en-las-afore-coloca-al-sistema-de-pensiones-a-la-vanguardia-tecnologica-del-sistema-financiero-31831?idiom=es . Consultado el 7 de julio

Les avatars sont une autre caractéristique fondamentale de notre identité numérique. Un avatar, mot d'origine française, peut avoir diverses significations.

Avatar[169] *: avatar [avataʀ] nom masculin*

(du sanskrit, proprement « descente »)

1. Dans la religion hindouiste, Chacune des incarnations du dieu Vishnou.

2. fig. Métamorphose, transformation.

3. abusivt Mésaventure, malheur.

4. ***Personnage virtuel choisi par un internaute pour le représenter dans l'univers des jeux en ligne.***

Dans le cadre de notre étude, nous retiendrons la dernière définition, qui se réfère à un personnage virtuel choisi par un internaute pour le représenter dans l'univers des jeux en ligne, cependant, en langue espagnole, cette définition n´est pas reconnue :

Avatar[170]

Du français avatar, provenant du sanscrit " avatâra" 'descente ou incarnation d´un dieu'.

1. m. Phase, changement, évènement imprévu.

2. m. Dans la religion indoue, incarnation terrestre d´une divinité, plus particulièrement Visnú.

3. m. Réincarnation, transformation.

De la même manière, le concept reprend l'idée de transformation, de devenir quelque chose de différent de ce qu'il est.

Précisément, les avatars sont cet ensemble d'éléments qui composent notre identité virtuelle. Cette identité que nous utilisons pour naviguer dans le monde numérique, la majorité du temps de manière licite, mais pas seulement. En effet, la création en soi d'une identité alternative n´est pas une activité illicite, cependant elle peut faciliter des activités considérées comme telles, car ces identités offrent à leurs créateurs un certain niveau d'anonymat.

[169] Avatar. *Diccionario Le Robert* 2017.
[170] *Avatar; Dictionnaire de la langue espagnole, (DRAE). Édición 23.ª, publiée en 2014.* Voir; http://dle.rae.es/?id=4X6SYjl consulté le 20 novembre 2017.

L'internaute vit de plus en plus sous de multiples identités numériques, la notion de pseudonymes, de contraction de pseudonyme et d'anonymat, est confortée par le fait de l'absence d'interaction physique des internautes.[171]

Cette identité numérique est la clé de notre étude, mais surtout c'est le point culminant de notre société d´'information. C'est également le souci des gouvernements qui craignent de ne pas pouvoir identifier de manière directe et précise les criminels informatiques qui profitent de ces circonstances.

Le paradoxe de cette multiplicité d'identités dans la vie pratique est qu´elle a été crée dans le but d´acquérir une certaine « liberté » d'action dans le monde numérique, mais qu´en réalité cette notion se réduit de plus en plus. Loin de se sentir libre, la gestion de tous nos identifiants numériques est de plus en plus difficile à contrôler, et c'est précisément cela qui met en péril nos identités numériques.

Au sein des concepts intrinsèques de l'identité numérique, il est important de définir et de les différencier les uns des autres, par exemple : les identités, les données d'identification et les données d'authentification.

Lorsque nous créons une identité numérique, nous passons par différentes étapes ou processus :

1. Inscription ou création d´identité ;
2. Vérification de la création du compte ou de l´identité ;
3. Identification ;
4. Authentification.

Par exemple, aujourd'hui nous avons une identité numérique dans le cadre professionnel nous avons un email, un utilisateur et un mot de passe de l'entreprise ; mais nous avons aussi une identité familiale pour communiquer avec les amis, la famille et les inconnus des réseaux sociaux. Le

[171] Iteanu, Olivier "L'identité numérique en question" Éditions Eyrolles, París, 2008.

thème spécifique des réseaux sociaux est très pertinent dans cette étude car de nos jours ils sont une partie essentielle de notre vie quotidienne.

Les réseaux sociaux font partie d'un univers bien plus vaste, que l'on appelle les médias sociaux en langue anglo-saxonne. Cet univers inclue tous les outils à travers lesquels un individu peut communiquer avec une infinité d´autres individus, dans pratiquement n'importe quelle partie du monde [172]. Les réseaux sociaux sont une série d'outils de contact social dans lesquels nous interagissons à travers un profil, réel ou imaginaire, avec un nom d´utilisateur, un alias ou avatar, qui lui-même peut se diviser en une série d'identifiants, par exemple : un profil Twitter se compose d´un nom d´ utilisateur, d´une biographie, d´une photographie ou d´un espace pour une image, d´un moyen de contact, et parfois même de la date de naissance, pour les utilisateurs qui le souhaitent.

Graphique. 1 Exemple d´un profil de Twitter

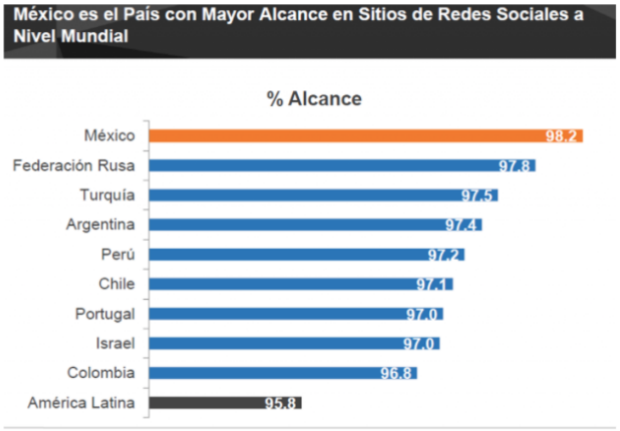
Dans d'autres réseaux sociaux beaucoup plus complexes, on recueille d´autres données d'identifiants qui peuvent même être considérées comme des données sensibles. Par exemple, Facebook ; l'information qui est exposée dans ce réseau social, si l´on analyse ne serait-ce que le formulaire de données personnelles, inclut des thèmes délicats et intimes comme la préférence sexuelle, la situation maritale, l'affiliation politique et même la religion, et bien d´autres informations qui s´accumulent quotidiennement.

L´intérêt de ces réseaux sociaux est qu'ils nous permettent d'interagir avec d'autres

[172] Mokhtari, Farah "*L'impact des réseaux sociaux*», Telecom Sud Paris. En: http://ima4505.wp.tem-tsp.eu/files/2012/03/impactreseauxsociaux.pdf consultado el 20 de septiembre de 2017.

personnes proches et éloignées, avec lesquelles nous pouvons avoir un nombre infini de relations de différents types. C´est là que naît un concept intéressant, connu comme la vie privée social, bien que cela semble contradictoire, l'être humain a ce droit à la confidentialité concernant ses données personnelles et en même temps, ce droit de « sortir de soi pour vivre avec les autres », qui doit être pleinement garanti, c'est-à-dire, respectez sa volonté de s´ inscrire sur un réseau social garantissant la protection et la confidentialité des données personnelles.

Rien qu´ 2014, le Mexique était le principal utilisateur des réseaux sociaux en Amérique latine et dans le monde, Facebook étant le réseau social le plus populaire :



Graphique. 2 Statistique de la Comscore, publiée par Forbes México.[173]

Dans le cas de la France, l'utilisation des réseaux sociaux depuis 2012 est en hausse comme le montre le graphique suivant :

[173] Méxique, premier pays de penetration dans le réseaux sociaux. Voir: https://www.forbes.com.mx/mexico-primer-lugar-en-penetracion-social-media/. Consulté le 30 septembre de 2014.

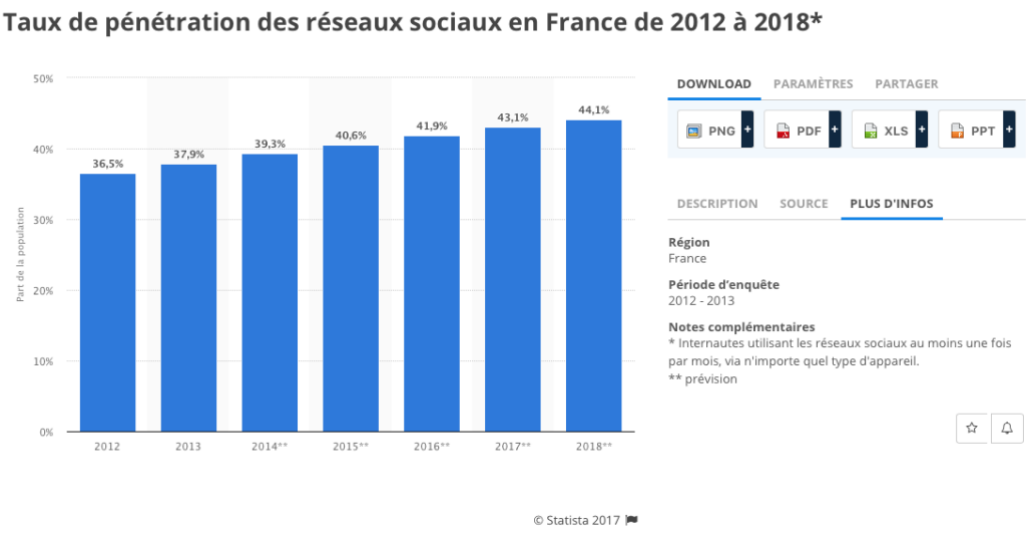


fig. 3 Taux de pénétration des réseaux sociaux en France de 2012 a 2013 et prévision à 2018[174].

Il est indéniable que la plupart des fournisseurs des réseaux sociaux les plus populaires du monde sont d'origine américaine. C´est pourquoi, lorsque l'utilisateur souscrit à ces réseaux sociaux, il adhère aux contrats stipulés par le fournisseur qui sont de nature civil et mercantile. Cependant, dans différents processus judiciaires, il a été prouvé que ces contrats violent plusieurs lois, et contiennent des clauses abusives et les utilisateurs de ces plates-formes se retrouvent sans défense.

Lorsqu'un utilisateur s'inscrit à un réseau social hébergé à l'étranger, ce contrat établie comme juridiction ce pays, généralement les États-Unis, en dépit du fait que selon les règles du droit civil et des principes de base des contrats, cela suffirait pour que les deux parties connaissent clairement leurs droits et exceptions. En effet, il existe des droits inaliénables, tels que les droits des consommateurs ou le droit à la vie privée et la protection des données personnelles.

La loi américaine permet l'existence de contrats réalisés par le biais de supports électroniques dans deux modalités différentes, le "click wrap" et le "browse wrap". Le premier exige que l'utilisateur remplisse une case ; le second consiste à ce que la seule visite du site par l´utilisateur sous-entend qu´il accepte les termes et conditions d'utilisation du site. Au Mexique, le Code civil

174 Taux de pénétration des réseaux sociaux en France de 2018-2018. En: https://fr.statista.com/statistiques/490928/utilisateurs-reseaux-sociaux-france/

fédéral reconnaît le consentement donné par voie électronique comme un consentement exprès. C´est grâce à ce type de mécanismes de présomption ou de preuve de l'expression du consentement, que la plupart des plates-formes de réseaux sociaux fonctionnent.

1.5 L´ IDENTITÉ SOCIALE

Puisque nous avons parlé du droit à la protection des données personnelles, il est important de commenter le droit de décider du niveau d'exposition sociale de l'individu, Celui-ci, est capable, au moins en théorie, de mesurer les risques cela implique, c´est à dire l'équilibre de deux concepts intéressants : la vie privée par *privacy by design* y sociability *by design*.

Le concept d'identité sociale apparaît à plusieurs reprises dans la jurisprudence de la Cour européenne des droits de l'homme. Cette identité s'oppose à l'identité physique, puisque l'identité sociale est une sorte de passeport qui reflète le meilleur de sa personnalité, c'est-à-dire du profil social, de ce qui nous permet de jouer un rôle dans la société d'information.

Ce profil devient une sorte de vitrine personnelle, à travers de laquelle l'utilisateur des réseaux sociaux décide librement ce qu'il veut révéler ou non, sa véritable identité et des caractéristiques les plus intimes de sa personnalité.

L'une des principales raisons pour lesquelles les gens deviennent dépendants de l'utilisation des réseaux sociaux est inhérente à la nécessité de partager et de coexister à travers cette interconnexion possible et favorisée par les nouvelles technologies. Les liens que l'utilisateur peut établir sont de nature diverse et peuvent donc avoir des connotations différentes pour lui, par exemple: donner ou recevoir un "*poke*"[175], un "*like*"[176] ou, plus récemment, exprimer une émotion spécifique à propos d'une publication en utilisant une "*émoticône*[177]", celle-ci ayant donné aux réseaux sociaux

[175] Poke, est une fonction du réseau social Facebook, qui permet, dans un certain sens, d´attirer l´attention de l´ utilisateur auquel on envoie le poke, meme si il peut s´interpreter comme une maniere de saluer, utilisé avec exces, il peut s´apparenter à un genre d´harcelelemnt-
Lien, Poke: la fonctionnalité de Facebook ne sert…. à rien. Voir: https://hipertextual.com/archivo/2010/07/poke-la-funcionalidad-de-facebook-que-sirve-para-nada/ consulté le 20 février 2015.

[176] J´aime, est une fonction du réseau social Facebook, à l´origine representée par une main avec le pouce levé, ce qui en langue anglo-saxonne se nomme "Thumbs up" et s´utilise comme signe d´approbation, ont ensuite été crée d´autre tipes d´emotions pour commenter la publication des utilisateurs.. Comme référence, consulter: https://elsemanario.com/hasta-el-momento/122803/video-likes-con-emociones-llegan-a-facebook/

[177] Emoticone est un neologisme créé à partir des mots emotions et icône, au pluriel emoticones. Dans certains pays et communautés Internet, on appelle emoticone (latinalisation du mot anglais « emtocon »), emoticone, icones gestuelle ou

un sens beaucoup plus intime et personnel. La société mexicaine, par exemple, est excessivement sensible au fait de recevoir ou pas l´'approbations ou une retro-alimentation à leurs publications. C´est tellement important que certaines personnes peuvent réellement souffrir d'anxiété ou d'angoisse à cause de l'indifférence de leurs amis de Facebook.

Une autre caractéristique intéressante à mettre en évidence des réseaux sociaux les plus populaires et qui implique clairement le traitement des données personnelles, pas toujours consenti par le propriétaire, est la fameuse *étiquette* ou tag, qui consiste à identifier les personnes ou utilisateurs, soit dans une publication ou directement sur une photographie. Ceci est un point particulièrement important car il n'y a pas d'autorisation *a priori* de la personne qui a été identifiée ou nommée. L'option qui est habituellement proposée est la possibilité de retirer cette étiquette ou faire qu'elle n'apparaisse pas dans la biographie- C´est une illustration très claire du système américain en ce qui concerne le traitement des données personnelles ou ce qu'on appelle un *opt out* qui suppose le consentement à moins que la personne concernée ne manifeste le contraire.

Enfin, avant de clore le sujet controversé des réseaux sociaux, nous citerons le dernier concept que nous considérons comme banalisé et pourtant dangereux, le terme *ami*. Sur Facebook, tous les utilisateurs qui font partie de votre liste de contacts, sont identifiés comme *amis*, sur Twitter, ils sont connus comme "Followers", ce qui est un concept moins intime. Le fait que ces personnes (réelles ou fictives) qui sont ajoutées à la liste des contacts de ce réseau social s'appelle *ami*[178], peut devenir une arme potentielle contre la vie privée et la sécurité des utilisateurs.

Les *concepts* traditionnels concernant les relations interpersonnelles des individus ont pris une autre dimension grâce aux réseaux sociaux. Par exemple, on peut supposer aujourd'hui qu'une relation amoureuse est formelle une fois qu´elle est annoncée en tant que telle sur Facebook. D´ailleurs, la jurisprudence française s´est prononcée en ce qui concerne la suppression du statut "*fiancé*" et pourrait engendrer des paiements des dommages et intérêts et préjudice moral.

L´intérêt de comprendre la portée de ce qui est si mal compris et imperceptible comme l´est notre identité numérique est de pouvoir mesurer les risques de notre exposition, de manière à pouvoir

masque. Voir: https://es.wikipedia.org/wiki/Emoticono Consultado el 20 de abril de 2017.

[178] [178]Gros, Marie-Joëlle, *Professeur, veux-tu être mon ami ?* En: http://www.liberation.fr/ecrans/2011/02/08/professeur-veux-tu-etre-mon-ami_955813 consultado del 23 de mayo de 2014.

limiter tout ce que nous partageons de nous-mêmes au monde entier.

CHAPITRE II.

LE PRINCIPE DE PROTECTION DES DONNÉES PERSONNELLES.

La protection des données personnelles est un concept à géométrie variable entre les trois pays qui font partie de notre étude, puisque les principes directeurs de ce droit ne prennent pas en compte les mêmes critères dans chacune des traditions juridiques. Alors qu'aux États-Unis, le principe de protection des données personnelles est très limité, en Europe, il s'agit d'une question très réglementée qui, par conséquent, donne lieu, en France, a des règlementations très claires en la matière. Dans le cas du Mexique, la législation respecte pleinement les critères européens pour la protection des données à caractère personnel, mais prévoit un système d'exceptions très précises qui la rendent compatible avec la réglementation américaine.

Nous allons commencer par étudier les États-Unis, car c'est le pays dont le système de protection est de loin plus souple.

2.1 LA PERCEPTION DES ÉTATS-UNIS SUR LA PROTECTION DES DONNÉES PERSONNELLESALES.

Aux États-Unis, historiquement et plus encore depuis le 11 septembre 2001[179], la priorité est à la sécurité nationale[180] bien plus qu´au droit à la vie privée. Il est important de prendre en compte que la protection constitutionnelle de ce droit est limité, la priorité étant à la sécurité et au bien-être de la nation dans son ensemble. Les citoyens américains peuvent invoquer la protection selon le quatrième amendement et la loi sur la protection des renseignements personnels, mais les droits de protection des données accordés dans le domaine de l'application des lois sont interprétées d'une manière limitée, avec une tendance générale à favoriser l'application de la loi et les intérêts de sécurité nationale; en particulier, tout ce qui concerne ou justifie l'échange et le transfert de renseignements personnels, même contre la volonté ou la méconnaissance de son propriétaire.

[179] *How has national security changed since 9/11/2001?* En: https://www.securitydegreehub.com/national-security-since-september-eleventh/ consultado el 11 de enero de 2017.
[180] Brown, Logan, *A Brief History of American National Security*. En: https://ivn.us/2014/03/24/a-brief-history-of-americas-approach-to-security/ consultado el 13 de septiembre de 2013.

2.2 LE SYSTÈME MEXICAIN DE PROTECTION DES DONNÉES PERSONNELLES

La protection des données personnelles au Mexique apparaît comme un besoin d'assimiler notre droit à celui de la société européenne, en partie à cause des accords de libre-échange et aussi pour faire face au besoin évident d´ une réglementation fédérale en la matière. Nous analyserons plus loin l'évolution de notre loi mexicaine sur la protection des données personnelles, mais après plus de dix ans notre loi fédérale sur la protection des données à caractère personnel en possession d'individus a enfin vu le jour telle comme nous la connaissons actuellement.

Le modèle dit *hybride* est le résultat d'intenses négociations dans les Chambres législatives et de l´influence de réglementations internationales telles que: Directive 95/46 / CE du Parlement européen, du Cadre de confidentialité du Forum de Coopération Économique d´Asie-Pacifique (APEC) , des Lignes directrices de l'OCDE sur la protection de la vie privée et des Flux Transfrontières de données à caractère personnel, de la Convention 108 du Conseil Européen sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, et des normes internationales pour la protection des données personnelles, en relation avec le Traitement des données personnelles (Résolution de Madrid).

Après débats sur les différents projets de loi, il a finalement été décidé de créer un modèle combinant le meilleur de chacune des dispositions susmentionnées. Les raisons sont nombreuses, l'une d'entre elles est économique puisque notre partenaire commercial le plus fort au moment des débats, était les États-Unis, et que sa législation est laxiste et sectorielle.

Il convenait de respecter les accords précédemment pactés lors de l'Accord de libre-échange Nord-Américain concernant la libre circulation transfrontalière des biens, services et capitaux, et les données personnelles qui vont de pair avec ces transactions. Cependant, il était essentiel d'avoir un cadre juridique en termes de protection de la vie privée et des données, et c'est ainsi qu´en négociant et jonglant avec les grands de l'industrie, les législateurs et la société civile ont créé un précédent mondial favorisant la protection. des données personnelles et le développement commercial du pays.

La loi mexicaine, tout comme la loi française, est basée sur les principes et les devoirs qui régissent le traitement des données personnelles, bien que ceux-ci soient beaucoup plus détaillés que dans la réglementation européenne.

Dans le domaine de la protection de l'identité, il est fondamental de lier chaque principe au droit à la protection de l'identité. Comme nous l'avons déjà mentionné, elle est constituée de données infinies à caractère personnel, qu´il s´agisse de celles qui donne naissance à l'individu comme le code génétique, ou de celles moins transcendantes, comme l'adresse ou le numéro de téléphone, sans oublier les données générées quotidiennement avec nos activités Internet, en particulier les métadonnées qui contiennent des références à chaque fois plus précises concernant notre identité.

La législation mexicaine reprend les principes directeurs de l'Union européenne et de la France et, d'une certaine façon, les détaille, en créant huit principes directeurs et deux devoirs ayant le même niveau d'applicabilité.

2.3 LES PRINCIPES DIRECTEURS DE LA PROTECTION DES DONNÉES PERSONNELLES EN FRANCE.

En France, la législation sur la protection des données personnelles est la Loi Informatique et des Libertés ou Loi n ° 78-17 du 6 janvier 1978 (LIL)181. Il convient de mentionner que ce texte a été modifié à de nombreuses reprises, de fait, la dernière réforme de 2017, a eu lieu suite à la réforme du règlement général européen sur la protection des données (GDPR)182.

La loi n ° 78-17 du 6 janvier 1978 est l'une des premières à réglementer le traitement des données personnelles en Europe. En vertu de l'article 2 de la loi susmentionnée, modifiée par la suite pour se conformer à la directive européenne de 1995, le champ d'application se limitait au traitement de données à caractère personnel effectué par des moyens automatisés ou non automatisés ou dont la vocation était intégrer les dossiers, à l'exception des données qui ont été recueillies et traitées à des fins exclusivement personnelles

Il y a des concepts de base que nous devons analyser avant l'étude des principes, puisqu'il est nécessaire de comprendre ce que la loi n ° 78-17 du 6 janvier 1978 entend par données personnelles, fichier et la portée du mot “traitement”.

[181] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[182] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation). En: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679. Consultado el 10 de diciembre de 2017.

Données personnelles[183]: En vertu de l'article 2 de la LIL, constitue une donnée personnelle, toute information relative à une personne physique identifiée ou pouvant être identifiée, directement ou indirectement, soit par son numéro d'identification, soit par un ou plusieurs éléments qui lui corresponde. Pour déterminer si une personne est identifiable dans ces termes, il doit considérer l'ensemble des moyens disponibles qui permettent son identification ou, auxquels la personne chargée du traitement ou toute autre personne peut avoir accès.

Il est important de souligner que même si les données personnelles traitées peuvent bénéficier d'un certain niveau d'anonymat, si cela peut être réversible, nous parlons alors de données personnelles. Pour être plus spécifiques et faire le lien avec notre objet d'identification, les données de géolocalisation[184] qui sont gardées dans un dispositif électronique, par exemple des données Waze qui sont sur iPhone, où l'utilisateur n'a jamais été signé ou ne s´est enregistré pour l´utiliser essayant de conserver son anonymat, pourraient dans un premier temps être considérées comme anonymes. Cependant, si celles-ci sont corrélées avec toutes les autres données du même dispositif, il est très probable que nous puissions connaitre l'identité de l'utilisateur dudit dispositif, c´est alors que les éléments d'identité de ce sujet pourraient être violés.

Il vaut la peine de préciser que différents critères doivent être remplis pour vraiment considérer qu'une personne puisse être identifiée. Il est vrai que les nouvelles technologies permettent la relation de gros volumes d'informations en un temps record, mais toutes les personnes ou entreprises n´ont pas le pouvoir économique de mener à bien cette activité. Il est donc toujours important d'effectuer une analyse rationnelle de la possibilité que cela se produise ou non.

Responsable : En vertu de l'article 3 de la LIL, la personne responsable du traitement des données à caractère personnel, sauf s´il est expressément désigné par la loi ou la règlementation, est la personne, l'autorité publique, le département ou l´organisme qui détermine les objectifs et moyens.

---

[183] *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.*
https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=3E9B9352377E9603D6ABF4D87BBC0DA3.tplgfr24s_2?idArticle=LEGIARTI000006528061&cidTexte=LEGITEXT000006068624&dateTexte=20180101

[184]

C'est-à-dire que c'est cette personne physique ou morale, de nature publique ou privée, qui décide du traitement des données personnelles.

Traitement : Le traitement est toute opération ou ensemble d'opérations liées aux données personnelles, quels que soient les moyens ou procédés utilisés, pour la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la communication par radio ou toute autre forme de disposition, de conciliation ou d'interconnexion, de blocage, d'élimination ou de destruction de ces informations.

Le concept susmentionné, extrait de l'article 2 de cette même loi, est le résultat des différentes réformes qui y ont été apportées, puisque le traitement des données à caractère personnel réglementées en tant que telles visaient initialement à créer des fichiers ou archives des utilisateurs. Cette définition élargie de la LIL, comprend maintenant tous les types de données personnelles, y compris ceux qui voyagent ou vivent sur Internet, et permet donc que cette loi leurs soient directement applicable.

Les types de traitement envisagés par la loi sont les suivants : traitement automatisé et non automatisé ; il est important de préciser que le simple fait que la manipulation d'un certain type d'informations effectuée au moyen d'un ordinateur n'implique pas directement le traitement des données personnelles automatisées. Il faudrait analyser dans un contexte global le type d'outils informatiques, leur fonctionnement, et la façon dont l'algorithme avec lequel ils ont été programmés gère l'information.

Dossier ou archive : il convient de noter que la traduction en langue espagnole du concept initial de fichier ne correspond pas exactement à ce que le LIL établit dans sa langue d'origine, la langue espagnole.

Dossier	Archive	Fichier
Du latin expediens, -entis, part.	Du latin archīvum, et du grec gr.	[fiʃje] nom masculin

act. de expedīre "lâcher", 'donner suite ', 'convenir'. 2. m. Sujet ou affaire suivie sans jugement contradictoire devant les tribunaux, à la demande d'une partie intéressée ou ex officio. 3. m. Ensemble de papiers correspondant à une affaire ou à une entreprise. Notamment utilisé pour mentionner la série ordonnée d'actions administratives, et aussi les poursuites judiciaires dans les actes de juridiction volontaire.	ἀρχεῖον archeîon. 1. m. Ensemble ordonné de documents qu'une personne, une société, une institution, etc., produisent dans l'exercice de leurs fonctions ou activités. 3. m. Action et fait d´archiver (‖ enregistrement de documents dans un fichier). Il a remis la documentation pour procéder à son archive. 5. m. Inform. Ensemble de données stockées dans la mémoire d'un ordinateur pouvant être manipulé avec une seule instruction.	1. Collection, réunion de fiches. — Inform. Ensemble structuré d'informations ; support de ces informations. 2. Meuble, boîte, classeur contenant des fiches.

Par conséquent, tout au long de ce travail, nous utiliserons le mot archive, que nous considérons plus précis et conforme à celui de la langue française et qui va dans le même sens que la LIL.

Les principes directeurs de la loi française sont principalement cinq, contrairement aux huit principes et dix devoirs de la législation mexicaine. Cependant, en réalité, les cinq piliers de la législation française sur la protection des données à caractère personnel envisagent, en pratique, toutes les obligations contenues dans la réglementation mexicaine, mais peut-être de manière moins détaillée.

CHAPITRE III :

LA MISE EN OEUVRE DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL : L'ETABLISSEMENT D´AUTORITÉS SPECIALES.

3.4 LES AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES DES ÉTATS-UNIS D'AMÉRIQUE.

Comme nous l'avons vu précédemment, l'un des grands problèmes du droit nord-américain en matière de protection des données personnelles est sa législation sectorielle et peu précise dans certains domaines. Cependant, un autre des grands problèmes de fond et d'application dont ils souffrent est le manque d´une autorité qui réglemente et sanctionne spécifiquement les actes qui violent la vie privée et la protection des renseignements personnels.

Cependant, de facto, la FTC, c'est-à-dire la Federal Trade Commission, est devenue l'Autorité de protection des données (DPA) des États-Unis par laquelle s´applique de manière agressive et sévère l'article 5 de la loi fédérale FTC, qui interdit les pratiques commerciales déloyales ou trompeuses. La FTC a accusé des entreprises victimes de violations de données par des pratiques commerciales déloyales ou trompeuses sous le motif que les infractions résultaient du fait que les entreprises n'adoptaient pas de mesures de sécurité raisonnables. Les entreprises que la FTC sous-entend couvrent l'ensemble des industries, des soins médicaux aux hôtels, les détaillants, les réseaux sociaux et autres sociétés Internet.

3.5 L´ INAI

Au Mexique, le droit à l'information est fondamental, exprimé dans le sixième article de la Constitution mexicaine. Avec l'alternance au pouvoir, se sont crées des espaces de participation citoyenne, ce qui a permis d'exiger que les actions gouvernementales rendent transparentes l'utilisation des ressources publiques. Le 11 juin 2002 a été signé le décret de promulgation de la Loi Fédérale sur la Transparence et l'Accès à l'Information Publique Gouvernementale, qui a donné naissance à l'Institut fédéral d'accès à l'information (IFAI).

L'histoire de l'IFAI, sa nature juridique, ses attributions et sa conception institutionnelle, sont inexorablement liées à la création de la Loi Fédérale sur la Transparence et l'Accès à l'Information Publique Gouvernementale au Mexique. Il convient donc de rappeler que, à l´origine, cette loi a été conçue pour être appliquée exclusivement dans le domaine de l'administration publique fédérale.

C'est au cours de son processus de discussion et de négociation qu'il a été décidé d'élargir son champ d'application pour y inclure tous les pouvoirs fédéraux et les organismes constitutionnels autonomes. Cependant, c'est également au cours de ce processus qu'il a été convenu d'établir et de concevoir en détail une autorité administrative dotée de l'autonomie opérationnelle,

budgétaire et de décision, chargée de promouvoir et de diffuser l'exercice du droit d'accès à l'information, de superviser la mise en œuvre de la loi et de résoudre les différends qui peuvent surgir entre les particuliers et l'administration publique fédérale en ce qui concerne les demandes d'accès à l'information et la protection de l'accès et de la rectification des données personnelles.

D'autres fonctions se sont ajoutées, ce qui a donné à l'IFAI un caractère particulier. En effet, ses attributions vont bien au-delà de la simple résolution des différends, puisque selon la loi, il correspond à l'organisme de réglementation en termes d'information et de protection des données personnelles pour l'administration publique fédérale, de surveiller le respect de la loi, de promouvoir l'exercice du droit d'accès à l'information parmi les citoyens et de susciter une nouvelle culture de la gestion de l'information, tant parmi les fonctionnaires que parmi les citoyens.

L'IFAI a été officiellement constitué, par décret présidentiel publié au Journal officiel de la Fédération le 24 décembre 2002, en tant qu'organisme décentralisé, non sectorisé, doté d´une personnalité juridique et de biens propres. Afin de garantir son autonomie budgétaire et administrative, elle est considérée comme une entité paraétatique de contrôle indirect qui n´est pas financée par un budget. En outre, il est précisé que l'organisme de contrôle interne ne peut pas intervenir dans les décisions de fond de l'Institut[185].

Le 7 février 2014 a été publié au Journal officiel de la Fédération, le décret réformant et ajoutant plusieurs dispositions de la Constitution politique des États-Unis du Mexique. En matière de transparence, les sujets obligés sont élargis afin d'exercer le droit d'accès à l'information publique, les bases sont posées pour articuler un Système National de Transparence, et l'autonomie constitutionnelle est accordée aux organismes garants fédéraux et étatiques, élargissant leurs pouvoirs et leurs compétences.

L'Institut national de la transparence, de l'accès à l'information et de la protection des données personnelles (INAI) est l'organisme constitutionnel autonome qui garantit le respect de deux droits fondamentaux : l'accès à l'information publique et la protection des données personnelles.

3.3 LA CNIL

185 185 Le futur de l´ ifai: considerations sur son autonomie constitutionelle. Voir: https://archivos.juridicas.unam.mx/www/bjv/libros/7/3196/2.pdf consulté le 14 mai 2016.

Pour assurer la mise en œuvre de la loi Informatique et Liberté de 197, une agence spécialisée a été créée : la Commission Nationale de l'Informatique et des Libertés (CNIL). À l´origine, la CNIL a été crée pour veiller au respect des dispositions de la loi précitée et, en particulier, d'informer les parties concernées de leurs droits et obligations. La Commission dispose d'un pouvoir réglementaire dans les cas prévus par la loi elle-même.

Il convient de rappeler que la loi, telle qu'elle a été conçue à l'origine, a dû être réformée afin de transposer la directive européenne de 1995 (95/46 / CE) à la législation française. Elle a donc été réformée en 2004 et parallèlement les pouvoirs et les facultés de la CNIL ont évolué. Le libellé original portait sur les procédures préalables à l'autorisation du traitement par la CNIL alors que le nouveau libellé établit un catalogue de contrôles et de sanctions.

Les pouvoirs de la CNIL passent d'être une série de contrôles applicables a *priori* à un contrôle *a posteriori*. Ce type de contrôles à pour but d'exercer son pouvoir de sanction sur plusieurs étapes.

Après avoir identifié un manquement aux obligations stipulées par la Loi, la CNIL peut mettre en garde la personne responsable du traitement afin qu'elle puisse corriger ladite non-conformité. Si le responsable ignore l´avertissement et n´initie pas des mesures nécessaires pour corriger la non-conformité, la CNIL peut imposer une sanction financière ou même empêcher ou arrêter le traitement des données selon la gravité de la menace et de ce qu'elle représente pour les droits et libertés des propriétaires de l'information.

La CNIL accompagne les professionnels pour qu´elles soient conformes aux lois et aide les personnes à contrôler leurs données personnelles et à exercer leurs droits. Elle analyse également l'impact des innovations technologiques et leurs immiscions dans la vie privée et les libertés. En outre, elle travaille en étroite collaboration avec ses homologues européens et internationaux pour développer une réglementation harmonisée.

CHAPITRE IV

SANCTIONS ET INFRACTIONS EN MATIÈRE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Les sanctions appliquées par chacune des autorités mentionnées dans le chapitre précédent

varient selon différents critères. Cependant, dans les trois cas les sanctions peuvent être élevées, financièrement parlant, indépendamment de l'atteinte possible à la réputation des entreprises en infraction. En effet, dans les trois différentes juridictions les infractions sont généralement d'intérêt public et la presse peut donc s´en emparer et les diffuser.

Une différence remarquable et intéressante est que, dans le cas du Mexique et de la France, c'est le Trésor national qui reçoit le montant des amendes, indépendamment de toute indemnisation qui peut être demandée par le propriétaire par un recours de droit civil, après avoir suivi le processus judiciaires correspondants. Aux États-Unis en revanche, la FTC a conclu des accords de coopération avec différents tribunaux civils et pénaux ce qui permet de poursuivre avec succès les contrevenants.

La Commission se concentre sur son programme de conformité à la loi, qui peut être complété par d'autres types de litiges. Le programme comprend des actions pour outrage civil, un programme de suivi et d´investigation des criminels et des procédures de recouvrement pour obtenir le paiement des jugements. Par conséquent, la FTC peut gérer les remboursements directs aux personnes affectées : une situation très bénéfique pour les citoyens américains.

Depuis l'entrée en vigueur du LFPDPPP entre janvier 2012 et juin 2016, le montant total des amendes infligées par l'INAI s'élevait à 235 millions 669 mille 887 pesos.

Les infractions les plus fréquentes et pour lesquelles des entreprises ou des particuliers ont eu une sanction économique sont : le traitement de données personnelles en violation des principes établis dans la Loi (légalité, information, responsabilité, loyauté et consentement) ; collecter ou transférer des données personnelles sans le consentement exprès des personnes, omettre l'avis de confidentialité, de la totalité ou d´une partie des éléments stipulés dans la norme.

Les procédures d'imposition des sanctions débutent au moment envisagé par la loi ou, le cas échéant, dés la fin des procédures de protection des droits.

Au 30 juin de cette année on comptait 185 demandes de protection des droits ARCO (accès, rectification, annulation et opposition). Il est important de souligner que dans

une même plainte, un ou plusieurs de ces droits peuvent être exercés.

De même, l'Institut a reçu 232 plaintes concernant la protection des données. 165 cas ont donné lieu à l´ouverture d'enquête préliminaire, 77 d´entre eux ont déjà été conclus et 88 restent en cours.

Parallèlement, l'INAI a mis en place 49 procédures de vérification afin de vérifier le respect de la loi et des règlements dérivés. 23 d´entre elles ont été conclues et 26 sont encore en cours.

Les cinq secteurs avec le plus grand nombre de vérifications sont les services financiers et d'assurance (15 procédures) ; de l'information dans les médias massifs et les services éducatifs (5 procédures chacun), et celui des services de soutien aux entreprises et autres services (4 procédures chacun).

Le statu *quo* de la CNIL en 2016 dévoile les conclusions suivantes :

En 2016, la CNIL a effectué 430 inspections *in situ*, sur demande, à propos de la documentation et des inspections en ligne. Approximativement 300 contrôles ont été effectués sur le terrain par une centaine de contrôles en ligne. Les audits sur les documents et sur demande, particulièrement adaptés aux organisations implantées hors de France, ont représenté une trentaine de missions.

La combinaison de différents modes d'intervention a été mise en œuvre avec succès dans de nombreuses missions qui ont détecté des violations en termes de protection des données (« brèches de sécurité » ou « fuites de données »). Après un contrôle en ligne et après avoir établi les test d'omissions, les agents autorisés se rendent dans l'organisation intéressée pour rechercher de nouvelles preuves. Une vingtaine d´opérations de la sorte ont été réalisées en 2016 et ont déjà donné lieu à quatre mises en garde, dont une publique.

20% des contrôles concernaient des dispositifs de vidéosurveillance installés dans des lieux ouverts au public soumis au code de sécurité interne.

SECONDE PARTIE

Les lois les plus sages ont pour but naturel d'entendre à tous les hommes les avantages de l'existence et de combattre tout ce qui tend à les concentrer sur un petit nombre et à accumuler d'un côté la puissance et le bonheur, et de l'autre la faiblesse et la misère.
Cesare Beccaria, 1764.

Internet donne accès à l'information et l´expression aux citoyens plus que tout autre moyen existant. La volatilité des sites et l'anonymat relatif propose un support qui favorise la liberté d´expression. Mais en vrai, Internet serait-il l'incarnation technologique de la célèbre bête de l'apocalypse?[186].

Nous ne pouvons pas diaboliser la technologie, mais il est vrai qu'Internet a ouvert les portes à des mondes et des comportements que nous ne connaissions pas et que nous avons tous ; utilisateurs, gouvernement, professionnels de la technologie et avocats ; dû apprendre en cours de route à preuves d´essais et d´erreurs.

L'expérience montre qu'une grande partie des juristes confrontée aux technologies de l'information, que se soient les avocats, législateurs ou juges, sont parfois perplexes devant le fonctionnement vertigineux, instable et presque mystique des réseaux et en général du monde informatique.

La différence culturelle et conceptuelle entre la science avec ses progrès technologiques et les principes généraux du droit, est devenue l'un des principaux obstacles contre le phénomène de la cybercriminalité. Les avocats doivent ouvrir leurs esprits à de nouvelles options et paradigmes qu´impose l'évolution technologique pour être en mesure de s´en servir afin de faire le bien et lutter contre le mal.

[186] Beson, Éric "La République numérique", Grasset, 2008

Le droit pénal appliqué aux technologies de l'information et de la communication est devenue un binôme de plus en plus fréquent malheureusement à cause de l'augmentation des activités illicites commises à travers ces nouveaux médias.

L'irruption du monde numérique dans nos vies et vice-versa a motivé une série d'éléments normatifs de nature criminelle. Le travail du droit criminel est la délimitation de cette frontière entre le bien et le mal, si ténue dans ce monde virtuel et qui passe parfois inaperçue sur Internet.

Au-delà d'une simple adaptation de l´architecture criminelle classique, où les rôles et les limites des comportements étaient parfaitement délimités, tous les acteurs doivent désormais s'adapter à un changement d'habitudes.

Un fait indéniable est que la loi pénale est confrontée à un nouvel environnement semi-inconnu mais qui ne peut être ignoré, le « cyberespace ».

Le crime est intimement lié à la manière d'être de chaque peuple et aux besoins de chaque époque. En effet, un fait considéré comme un délit à une certaine époque ou dans un certain pays, peut, dans d´autres circonstances ou de par l´évolution des mœurs et des us, être considéré comme licite[187].

1.1 LA CIBERCRIMINALITÉ

Le concept de cybercriminalité n'est pas suffisamment clair pour les autorités à niveau international. Le préfixe "cyber" vient d'un mot grec kubernan, qui signifie gouverner et également présent dans le mot cybernétique[188].

---

[187] Castellanos, Fernando “Lineamientos elementales de Derecho Penal”, Porrúa 1990, México. P. 125.

[188] Sobre la cibernética, hay al menos una cosa en la que todos están de acuerdo: esta palabra deriva de una palabra griega, *kubernêtik*ê, que Platón solía referirse al pilotaje de un barco. A menudo ha usado esta metáfora para presentar el verdadero arte de gobernar, el basado en la sabiduría, en el conocimiento del bien.

"La cibernética es el arte de hacer efectiva la acción". Esta definición de Couffignal, un pionero francés de la cibernética, es la más cercana a la concepción de Platón. El buen piloto es aquel cuya acción es efectiva en la tormenta. "Ciencia del control y la comunicación en los animales y la máquina. Esta es la definición de Norbert Wiener, el autor Cibernética o control y comunicación en el animal y la máquina, un libro publicado en 1948. A este estadounidense le atribuimos la

Ce préfixe « cyber » accompagne de nombreux mots contemporains que les internautes utilisent quotidiennement, tels que le cyberami, cybercafé, cyberfiancé, cyberattaques, etc.

De plus, ce préfixe est la base du mot qui nous préoccupe : la cybercriminalité. Celle-ci s´ associe à la criminalité réalisée par des moyens informatisés. De nos jours, on l´utilise pour dénommer diverses activités criminelles comme la cyberfraude, le ciberbullying ou le ciberterrorisme.

La cybercriminalité continue d'être une notion abstraite pour les juristes, puisque même la Convention sur la cybercriminalité du Conseil de l'Europe[189] ne la définit pas clairement, bien qu'elle définisse les diverses conduites illicites qu´encadre ce concept.

Le terme cybercriminalité défini par Interpol est le suivant :

"La cybercriminalité est un type de criminalité en croissance rapide. De plus en plus de criminels exploitent la vitesse, le confort et l'anonymat d'Internet pour commettre une variété d'activités criminelles qui ne connaissent pas de frontières, ce type de crime, physique ou virtuel, cause de graves dommages et constitue des menaces réelles pour les victimes dans le monde entier.

Bien qu'il n´existe pas de définition universelle unique de la cybercriminalité, l'application de la loi distingue généralement deux types de crimes liés à Internet :

La cybercriminalité avancée (ou crime de haute technologie) : attaques sophistiquées contre le disque dur et les logiciels d´un ordinateur ;

Crimes informatiques : des crimes « traditionnels » qui ont pris une nouvelle

paternidad de la cibernética. En: http://agora.qc.ca/dossiers/Cybernetique. Consultado el 20 de marzo de 2015.

[189] Convenio sobre la Ciberdelincuencia del Consejo de Europa, o Convención de Budapest del 23 de noviembre de 2001. En: https://rm.coe.int/16802fa41c. Consultado el 21 de marzo de 2015.

direction avec l'avènement d'Internet, tels que les crimes contre les enfants, les crimes financiers et même le terrorisme.

Les organisations criminelles se tournent vers Internet pour faciliter leurs activités et maximiser leurs profits en temps records. Les crimes en eux-mêmes ne sont pas nécessairement nouveaux, tels que le vol, la fraude, le jeu illégal, mais ils sont de plus en plus répandus et plus dommageables. "

Du point de vue français, une cyberattaque est définie par le gouvernement français comme :

Une cyberattaque est une tentative d'attaque des systèmes informatiques à des fins malveillantes. Il peut viser à voler des données, détruire, endommager le fonctionnement normal des appareils informatiques, prendre le contrôle des processus informatiques ou des dispositifs d'authentification trompeurs pour effectuer des opérations illégitimes[190]*. "*

Miguel Ángel Davara définie le délit numérique comme *"...'une action, réunissant les caractéristiques définies dans la notion de crime, réalisée par le biais d´un outil informatique, ou en violation des droits du propriétaire d'un élément informatique, qu'il s'agisse de disque dur ou de logiciel ".*

En droit mexicain, ces comportements illégaux ont été traités à un niveau doctrinal. Le code pénal de l'État de Sinaloa a été le premier à inclure dans son catalogue le terme de crime informatique, et bien que la définition soit encore très sommaire, on peut le considérer comme un précédent important en matière d'innovation législative.

1.2. LES DIFFÉRENTS VISAGES DE L'USURPATION DE L'IDENTITÉ.

En dépit du fait que la pratique du comportement illégal que nous connaissons aujourd'hui comme usurpation ou vol d'identité est assez ancienne, le Mexique et le monde entier ont tournés leur regard vers ce problème pour deux raisons principales : les grandes pertes économiques et la multiplication croissante des cas.

[190] Cyberattaque. En: http://www.gouvernement.fr/risques/lexique/lettre_c#parentVerticalTab16. Consultado el 25 de noviembre de 2017.

Comme nous l'avons souligné dans le paragraphe précédent, ce comportement illégal, tel qu´il est reconnu universellement, est un fait contraire à la morale, un manque d'éthique ou un fait interdit par la Loi. Ce n'est certes pas un comportement nouveau, cependant, il a connu un essor plus important grâce aux nouvelles technologies. Sa réalisation est devenue plus rapide et plus simple, et d'autre part, grâce à la technologie, il est aussi plus facile et plus rapide de découvrir une attaque de cette nature et de la dénoncer.

Comme nous l'avons expliqué précédemment, ce que nous connaissons comme « identité » est composé de facteurs très divers : légaux, physiologiques, génétiques, historiques, psychologiques et même spirituels ou religieux. Tous ces éléments contribuent à nous individualiser et nous identifier, en nous différenciant des autres au sein de la société dans laquelle nous nous développons. La question du vol d'identité est de plus en plus pertinente d'abord par sa tendance à croître dans toutes les parties du monde, et ensuite et surement la raison la plus importante, à cause de tous les biens juridiques qui deviennent vulnérables à cause de cet acte illicite.

L'identité est sans aucun doute composée de divers éléments, caractéristiques, références, documents, informations, données personnelles, habitudes, mots de passe, qui nous donnent accès à un certain nombre de droits, privilèges, activités, lieux, etc. D'une certaine manière, notre identité marque et définit notre place dans le monde, c'est pourquoi elle de plus en plus attrayante pour les criminels ou les délinquants : c'est une porte entre-ouverte sur notre monde. Du nombre d´informations que collecte le criminel dépend l´opportunité d´entrer dans notre monde et donc le degré auquel il peut nous affecter.

Légalement, l'identité est réglementée et protégée par les traités internationaux des droits de l'homme et bien sûr la législation des trois pays analysés dans cette étude. Par la déclaration des Droits de l'Homme et du Citoyen de 178, les droits naturels, inaliénables et sacrés de l'Homme ; tel est le cas du droit ou de l'identité personnelle sont reconnus par une déclaration solennelle.

La Déclaration des droits de l´homme

Depuis 1488 aux Etats-Unis

Ce que nous décrirons ci-après comme vol, supplantation ou usurpation d'identité est en soi une activité illicite qui ne vient jamais seule, c'est-à-dire qu'il y a toujours un moment avant

et après l´exécution du crime. Dans un premier temps, il s´agit d´obtenir des informations de manière licite ou non. Analysons cet exemple: On ne peut pas considérer de la même manière un criminel qui obtient les identifiants d'une personne en l´agressant dans la rue et en lui volant son portefeuille, que l´employé d'une société de services de téléphonie qui obtient légitimement une série d'identificants nécessaires à la réalisation d'un contrat de service et qui, par la suite, utilise de manière illicite cette information usurpant l'identité de la victime pour commettre un acte illégal, quelque soit sa nature.

En tout état de cause, il ne s'agit pas d'une conduite illicite isolée, puisque dès le moment où un sujet prémédite l'usurpation d'identité, c´est dans la majorité des cas pour commettre un autre crime qu´il ne pourrait pas commettre s'il n´avait pas voler antérieurement l´identité de quelqu´un.

À niveau international, en particulier dans les pays qui font partie cette étude, les comportements illicites que nous décrivons peuvent être dénommés de différentes manières, cités ci-dessous :

4. Usurpation d´identité ;
5. Vol d´identité ;
6. Supplantation d´identité.

Nous procéderons à l'analyse de chacun des termes cités, afin de déterminer celui que nous considérons le plus approprié pour décrire avec précision ce comportement. Même si cela peut paraitre superflu ou informel, en réalité c´est extrêmement important car si le concept ne répond pas d'une manière pertinente à la nature du comportement, il est très probable que non seulement les juges, mais aussi les législateurs des nouvelles générations ne puissent pas incorporer ce type de crime dans les diverses lois ou, le cas échéant, imposer des sanctions administratives pour les actes tendant à la perpétration de ce crime.

En premier lieu, nous allons analyser le concept de vol d'identité qui apparaît dans différents types criminels et est inclue dans les codes pénaux mexicains et dans le code pénal français. Nous allons clarifier ce concept pour en comprendre ses nuances.

Le terme usurpation, vient du latin *usurpatio*, qui tient ses origines du droit romain,

et est intimement lié au patrimoine, à la possession d´une propriété généralement immobilière. Nous nous confrontons alors à un premier dilemme puisque, comme nous l'avons expliqué ci-dessus, l'identité en tant qu'ensemble complexe ne peut pas être considérée comme une propriété mobilière ou immobilière. Le droit de propriété lui donnerait un caractère de « chose », mais il s´agit en fait plus d´un droit humain et personnel. D´un point de vue personnel, considérer l´identité comme une chose réduirait la gravité du dommage causé à la victime, hors ce n´a pas une conséquence seulement monétaire ou patrimoniale, mais cela a aussi des répercutions psychologiques et dans bien des cas physiques.

Un autre point important est la définition que nous donnons à « usurpation d'identité » : dans la plupart des cas nous nous référons à « l´usurpation d´identifiant ou de documents d'identification personnels » et non à l'identité elle-même. Par exemple, lorsqu'une personne utilise la carte de crédit de quelqun d´autre sans son consentement, ou la clône pour faire des achats en son nom et à son insu, il s´agit d´une utilisation illégale d'un moyen paiement et donc d´une fraude à un tiers par l´utilisation d'un instrument qui devrait être entre les mains de son propriétaire légitime. Cependant cela ne signifie pas que le criminel a pris pleine possession de la personnalité de sa victime, mais seulement de l´un de ses moyens de paiement ou identifiant bancaire dans un but précis qui n´ empêche pas la victime de continuer à utiliser sa propre identité. C´est souvent la raison pour laquelle la victime se rend compte bien plus tard qu´elle a été abusée et peut même avoir utilisé sa carte de crédit dans un autre établissement en même temps que le criminel.

Le pouvoir qu´octroie la connaissance des identifiants d´une personne, que ce soit dans le monde réel ou virtuel, dépend du type d'attaque. Par exemple, lorsqu'une personne est victime d'une attaque de phishing, c´est à dire le partage de son mot de passe sur un réseau social tel que Facebook, les criminels peuvent prendre le contrôle du compte et publier en son nom. Cela dit, ce contrôle ne fait référence qu'à l'un des identifiants virtuels de la victime et non à son identité en soi : Pedro López reste Pedro López et ne perd aucun des attributs de sa personnalité ou de son identité pour avoir perdu ou donné le contrôle de son identité virtuelle sur Facebook. Dans la plupart des cas lorsque la victime découvre rapidement qu´elle a été attaquée et grâce aux politiques privées de la plate-forme elle-même, elle peut reprendre le contrôle de son compte dans un délai raisonnable.

Nous nous penchons sur cette réflexion car nous cherchons encore une fois à ce que le nom donné à cet acte illicite soit le plus précis et approprié à la nature du comportement et à ses éléments caractéristiques.

L'usurpation est définie par l'Académie royale espagnole comme :

> "1. f. Action et fait d'usurper.
> 2. f. La chose usurpée, plus particulièrement le terrain usurpé
> **3. f. Der. Crime commis par l´appropriation, par la violence ou l'intimidation, de la propriété ou du droit de propriété d'autrui"**

Par conséquent, la dernière définition nous renvoie inévitablement au domaine des droits de propriété, c'est-à-dire à celui qui traite d'une chose, dans ce cas d´un bien immobilier. On entend donc par identifiants ou documents d'identifications, une chose et en particulier, de par sa nature, un bien comparable à un meuble en vertu de l'article 759 du Code civil fédéral : le terme usurpation serait donc incorrect.

Cependant, au Mexique, le terme usurpation d'identité est reconnu comme correct, tant et si bien qu´ il est classé dans les lois pénales d'État suivantes :

Chapitre III du Titre Douzième du Code pénal du District fédéral des Crimes contre la paix, la sécurité des personnes et l'inviolabilité du domicile, le type d'usurpation d'identité criminelle étant la suivante :

> ***Article 211 Bis***. - *Qui usurpe, à des fins illicites, l'identité d'une autre personne, ou donne son consentement à l'usurpation de son identité, sera puni d'une peine de un à cinq ans de prison et d´une amende allant de de quatre cents à six cents jours de salaire minimum.*
>
> *Les peines prévues à l'alinéa précédent seront majorées d'un tiers à l'égard de ceux qui usent d'homonymie, la ressemblance physique ou la similitude de voix pour commettre l'infraction établie dans cet article.*

Selon l'article précédemment cité, le comportement illégal consiste à usurper l'identité d'un autre à condition que se soit à des fins illicites. Il sous-entend alors la possibilité que se soit fait dans un but licite : il ne pourrait s´agir que d´une raison de vie ou de mort ou d'intégrité humaine, cas difficilement possible ou envisageable. L´article stipule également que le sujet actif est aussi

celui qui autorise un tiers à supplanter son identité. Enfin, il envisage une peine aggravante en cas d´utilisation d'homonymie, de ressemblance physique ou de similitude de la voix pour commettre le crime, c'est-à-dire par l´utilisation d'éléments qui mettent le criminel en position d'avantage face à la victime.

3. Code Pénal dans l´Etat de Mexico

Le code pénal de l'État de Mexico reconnaît également l´usurpation d'identité comme un comportement illégal, le décrivant comme suit :

> ***Article 264***.- *Une peine de un an à quatre ans d'emprisonnement et une amende de cent à cinq cent jours de salaire minimum sera imposée à quiconque exerce un droit à des fins illicites ou utilise tout type de données, d'informations ou de documents qui appartiennent légitimement à un autre, qui l'identifie devant la société et lui permet, en tant que personne physique ou entité juridique collective, de se faire passer ou de représenter cette entité.*
>
> *Ces actes seront assimilés à un vol d'identité et les mêmes peines prévues au paragraphe précédent cet article seront imposées à ceux qui :*
>
> *I. Commettent un acte illicite prévu dans les dispositions légales pour condamner l'usurpation de l'identité*
>
> *II. Utilisent des données personnelles, sans le consentement de la personne qui devrait l'accorder*
>
> *III. Accordent leur consentement à l'usurpation de leur propre identité ; et*
>
> *IV. Se servent de l'homonymie pour commettre un acte illégal*
>
> *Les sanctions prévues dans cet article seront imposées indépendamment de celles qui correspondent à l´exécution d'un ou plusieurs autres crimes.*
>
> ***Article 265***.- *Les peines indiquées dans l'article précédent seront majorées jusqu'à la moitié, lorsque le crime est commis par un fonctionnaire qui profite de ses fonctions, ou à qui utilisent leur profession ou emploi*

à cet effet.

Nous ne devons pas nous surprendre de la manière dont ce législateur de Colima aborde ce problème objectivement et d'un autre point de vue, peut-être plus pratique, à ce que nous appelons généralement l´usurpation d'identité. En l'occurrence le code pénal de l'État de Colima assimile ce comportement à la fraude de la manière décrite ci-dessous :

> ***Article 201***. *Il est considéré comme une fraude et sera passible de quatre à onze ans de prison et une amende de quatre cent cinquante à mille jours de salaire minimum, dans les cas suivants :*
>
> ***… III. Utilisation incorrecte des cartes de paiement électroniques et des identifiants de paiement électronique.*** *Qui, sans le consentement du propriétaire ou de quiconque est autorisé à l´accorder, utilise une carte, un titre, un document ou un instrument de paiement électronique soit pour le retrait en espèces, soit pour le paiement de biens et de services.*
>
> .
>
> *La même pénalité sera imposée à ceux qui, avec le consentement du propriétaire ou de la personne autorisée à l´accorder, utiliseront de manière illicite les cartes, titres, documents ou instruments de paiement électroniques soit pour le retrait en espèces, soit pour le paiement de biens et de services*
>
> ***VI. Utilisation abusive d'informations confidentielles ou secrètes de cartes, de titres, de documents ou d'instruments de paiement de biens et services ou pour le retrait en espèces.*** *Celui qui obtient un profit au détriment du titulaire d'une carte, titre, document ou instrument de paiement électronique de biens et services ou pour le retrait d'espèces, par l'utilisation d'informations confidentielles ou secrètes de l'institution ou de la personne légalement autorisée.*
>
> *Si le sujet actif est employé ou dépend de la partie offensée, la peine d'emprisonnement passera de deux à cinq ans.*
>
> ***VII. Utilisation abusive d'un ordinateur.*** *Qui, pour toute utilisation des moyens informatiques, télématiques ou électroniques, réalise un*

profit pour lui-même ou pour autrui, par des manœuvres informatiques, instructions de code, prédiction, interception d'envoi de données, ajout de données, utilisation d´un réseau de sites miroirs ou de pièges pour collecter des informations cruciales afin d´utiliser de manière non autorisée les données, de supplanter une identité, modifier de façon indirecte par des programmes automatisés, image, courrier ou vulnérabilité du système d'exploitation, de tous les fichiers principaux, secondaires et tertiaires du système d'exploitation qui affectent la fiabilité et la navigation sur le net ou l´utilisation d´ un appareil similaire pour obtenir ce profit.

De même, la même sanction que celle du paragraphe précédent sera imposée à quiconque intercepte, interfère, reçoit, utilise, altère, endommage ou détruit un logiciel ou un programme informatique ou les données qu'il contient, dans la base de données, le système ou le réseau.

Dans le cas où l'actif possède une licence, un diplôme d'ingénieur ou tout autre diplôme universitaire reconnu dans le domaine de l'informatique, de la télématique ou de ses domaines connexes, la peine sera majorée jusqu´à quatre ans de plus de prison, en plus d´une interdiction ou suspension à exercer sa profession pour une durée égale à la peine d'emprisonnement imposée.

En fin de compte le législateur de Colima parvient à percevoir que le but ultime du délinquant qui supplante l'identité d'un autre en profitant de ses informations personnelles, comme ses identifiants, est de commettre un acte frauduleux qui lui génère un profit quel qu'il soit. Cela confirme que le but du sujet actif n'est pas en soi la supplantation d'identité, mais ce qu´il peut en obtenir, commettant ainsi une multiplicité d´actes illicites.

Pour la loi anglo-saxonne, le vol d'identité ou la fraude d'identité est précisément une nouvelle sorte de fraude, différente, mais une fraude quand même.

¿ Qu'est-ce que le vol d'identité et la fraude d'identité ?

Le vol d'identité et la fraude d'identité sont des termes utilisés pour désigner tous

les types de crimes dans lesquels quelqu'un obtient et utilise les données personnelles d'autrui d'une manière qui implique la fraude ou la tromperie, généralement à des fins lucratives.

Beaucoup de gens répondent au « spam » ou courrier électronique non sollicité qui leur promet un certain bénéfice, mais exige des données d'identification, sans se rendre compte que dans de nombreux cas l´expéditeur n'a pas l'intention de tenir sa promesse. Preuve que ans certains cas, les criminels ont utilisé la technologie informatique pour voler de grandes quantités de données personnelles.

Avec suffisamment d'informations d'identifiants d´une personne, un délinquant peut prendre en charge l'identité de cette personne pour mener à bien un large éventail de crimes. Par exemple :

- Demandes de prêts et de cartes de crédit,
- Retraits frauduleux de comptes bancaires,
- Obtenir tout type de privilèges auxquels il n'a pas droit.

Il existe plusieurs types de vol d'identité courants détectés aux États-Unis :

Vol d'identité des mineurs : les identifications des enfants sont vulnérables car leur vol peut passer inaperçu pendant de nombreuses années et lorsqu´ils sont adultes et se rendent compte, les dommages à leur identité ont déjà été commis.

Vol d'identification fiscale : Un voleur utilise votre numéro de sécurité sociale pour présenter de fausses déclarations d'impôt au Service des Impôts ou au gouvernement de l'État.

Vol d'identité médicale - Cette forme de vol d'identité se produit lorsque quelqu'un vole vos renseignements personnels, tels que votre numéro de Medicare [191] ou d'assurance-maladie, pour obtenir ces soins ou pour émettre une facture frauduleuse à votre fournisseur d'assurance-santé.

[191] [191] Medicare est le programme fédéral de sécurité sociale des États-Unis d'Amérique, pour les personnes âgées d'au moins 65 ans, les personnes plus jeunes handicapées et les personnes souffrant d'IRT (insuffisance rénale chronique nécessitant une dialyse ou une transplantation, parfois appelée IRT) .

Vol d'identité des personnes âgées : vol d'identité ciblant les personnes âgées. Les personnes âgées sont vulnérables au vol d'identité parce qu'elles sont en contact plus fréquent avec les professionnels de santé qui ont accès à leur information d'assurance-maladie, ou parce que les soignants et le personnel des établissements de soins de longue durée ont accès à des renseignements personnels ou leurs documents financiers, ou encore parce qu´elles ne savent pas manipuler correctement les nouvelles technologies.

Vol d'identité sociale : Un voleur utilise votre nom, photos et autres informations personnelles pour créer un faux compte sur une plate-forme de médias sociaux.

Le ministère de la Justice des États-Unis traite les cas de vol d'identité et de fraude en vertu de diverses lois fédérales. En l'automne 1998, par exemple, le Congrès a adopté la Loi sur le vol d'identité et la présomption de dissuasion suppositions (Identity Theft and Assumption Deterrence Act) ITADA[192]. Cette législation a créé un nouveau délit de vol d'identité, qui interdit de « transférer intentionnellement ou d'utiliser, sans autorisation, un moyen d'identification d´ une autre personne avec l'intention de commettre, d'aider ou d'encourager toute activité illégale. Ceci constitue une violation de la loi fédérale, ou constitue un crime en vertu de toute loi d´État ou locale applicable. "18 USC § 1028 (a) (7) Ce crime, dans la plupart des circonstances, entraine une durée maximale de 15 ans d'emprisonnement, une amende et la confiscation pénale de tout bien personnel utilisé ou destiné à être utilisé pour commettre le crime.

Dans la législation française, cette activité illicite est également reconnue, puisque depuis 2005 la criminalité liée aux moyens d'identification est devenue le dénominateur commun des autres crimes.

Pour l'auteur Guy de Felcourt, il existe différents phénomènes qui contribuent à l'augmentation de ces fraudes liées à l'identité, l'une des plus importantes : l'ingénierie sociale, comprise comme l'art de la manipulation humaine exercée dans l'intention de mener à bien des activités frauduleuses ou de divulguer des informations confidentielles ou secrètes de la victime. Cela peut se produire en ligne ou en intimidant personnellement l'individu, qui est sans aucun doute le maillon le plus faible.

[192] *Identity Theft and Assumption Deterrence Act*. Voir: https://www.ftc.gov/node/119459. Consulté le 11 novembre 2016.

Comme nous l'avons supposé tout au long de ce travail, l´usurpation d'identité n'est pas un comportement nouveau, nous pouvons même dire qu'il remonte aux origines de l'être humain.

L'identité personnelle est liée à des phénomènes sociologiques et psychologiques, au besoin d'être reconnu, individualisé et estimé par l'environnement social.

Historiquement, l'usurpation d'identité apparaît déjà dans la mythologie égyptienne, grecque et romaine. D´ailleurs, même le mot hypocrisie, d'origine grecque, signifie prétendre être ou sentir quelque chose contraire à la réalité, l'art de l'apparence.

Si la question a été abordée avec beaucoup plus d'intérêt, c'est à cause ses graves conséquences économiques et la France n'y a pas échappé.

Avant 2011, en France, l'usurpation d'identité ne constituait pas un crime en soi. Au jour d´aujourd´hui, le Code pénal l´envisage depuis la création de la loi n ° 2011-267 du 14 mars 2011 d'orientation et de programmation pour l'amélioration de sécurité interne, mieux connu sous le nom de LOPSI

L'article 226-4-1 stipule :

> *“ Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.*
>
> *Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.*

Nous avons déjà parlé des droits de la personnalité et de la reconnaissance des biens moraux dans le Droit Civil moderne dans lequel est reconnu la figure du dommage moral.

On considère comme un dommage, une perte ou une altération, une détérioration, une offense ou une douleur qui est causée à une personne, une chose ou les objets de valeurs dont une personne est le propriétaire.

En ce sens, lorsqu'un bien est violé, cette atteinte n'implique pas seulement des

aspects économiques mais aussi moraux, comme les cas que nous avons exposés précédemment, où la victime souffre de dommages psychologiques et émotionnels, souvent irréparables car ceux-ci bouleverse des domaines aussi intimes que la dignité, l'intégrité ou l'image de soi.

C´est ainsi que nait le besoin de créer une figure qui permette d'indemniser ou de réparer d'une manière ou d'une autre les dommages subis dans les biens économiques ou moraux des victimes.

Le préjudice moral est une action de nature civile reconnue par les trois législations analysées dans cette thèse. Le droit français est pionnier dans ce domaine, suivi du droit anglo-saxon et du droit mexicain.

Ainsi, le droit civil entre en action lorsque, par la violation de l'identité ou de la vie privée ou des données personnelles, la victime subit une sorte de dommage économique ou moral et cherche une réparation éventuelle.

L'exercice de ce droit suit des critères différents selon les pays.

En France[193], pour permettre la demande d'indemnisation, un dossier doit être dûment constitué et la victime doit évaluer le montant de la réparation (y compris les coûts directement liés au dommage subi).

La législation américaine prend exemple sur le droit français et est donc fondée sur des critères similaires. Cependant dans la pratique, il existe certains cas où des sommes exorbitantes ont été exigées sur la base de faits et de raisonnements qui ne sont pas toujours objectifs.

Lorsqu'un préjudice résulte d'une action négligente ou malveillante d'une personne envers une autre personne, celle qui a subi le préjudice peut réclamer des dommage et intérêts sous la forme d'une compensation monétaire. Le jury ou le juge exerce un large pouvoir discrétionnaire pour accorder des dommage et intérêts compensatoires en matière de dommages moraux. La mesure des dommages compensatoires doit être réelle et tangible. Il est difficile de fixer un montant avec

[193] La responsabilité extracontractuelle en général. En : https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721&idSectionTA=LEGISCTA000032021488 Consulté le 12 novembre 2017

exactitude lorsqu´il s´agit de douleur, souffrance ou détresse émotionnelle. Lors de l'évaluation du montant des dommages et intérêts compensatoires qui seront accordés, le juge ou le jury doit faire preuve de discernement et de bon sens, en se fondant sur l'expérience générale et la connaissance de l'économie et de l'environnement social. Cependant, une décision appropriée serait fondée sur des preuves substantielles.

La douleur et la souffrance sont un motif approprié pour avoir une compensation monétaire pour les dommages causés par un acte de négligence ou d´omission.

CONCLUSION DE LA DEUXIÈME PARTIE.

La société de l'information et la manière dont laquelle nous nous y mouvons ont entraîné une série de défis législatifs pour les pays et les autorités qui doivent faire face à de nouvelles façons de commettre des actes illicites, qu'ils soient criminels, administratifs ou civils. Il faudrait se convertir en une sorte de magicien pour faire face à ces défis légaux qui épuisent les ressources de toutes les instances existantes, le chemin criminel n'étant pas toujours l'idéal ni le plus simple. Il est temps de considérer la protection de l'identité numérique comme un appareil juridique holistique qui devra s´appuyer sur les différentes branches de la loi pour sauvegarder les droits de la victime et indemniser autant que possible les dommages.

TROISIÈME PARTIE : L'IDENTITÉ NUMÉRIQUE EN TANT QUE SOURCE D'ÉVOLUTION DU DROIT

CHAPITRE I : L'ÉVOLUTION DE LA PROTECTION DE L'IDENTITÉ NUMÉRIQUE COMME ENSEMBLE DE DONNÉES PERSONNELLES.

Nous avons abordé la question de la personnalité et dans ce contexte s´est dégagé le concept d'identité ou plutôt, l'ensemble des identifiants qui permettent à une personne d'être présente dans le monde, de faire sa vie quotidienne et sa routine. Nous allons maintenant analyser plus précisément et fermement la question de l'identité numérique.

De même, un effort a été fait pour conceptualiser l'identité numérique. Nous considèrerons l’identité numérique comme l'ensemble des éléments d'identification qui servent à une personne physique, morale ou entité gouvernementale, pour se distinguer des autres dans un

environnement numérique ou virtuel, soit pour construire une réputation numérique, communiquer, avoir des relations, acquérir des droits et des obligations face à d'autres utilisateurs ou seulement pour être plus visible dans les médias informatiques.

L'identité numérique est un paradoxe d'éléments qui peuvent à leur tour servir d'identifiants et d'outils pour rendre anonyme. C'est-à-dire que si certaines personnes physiques ou morales utilisent ces éléments d'individualisation dans le but d´une personnalisation ou pour transférer leur identité réelle ou collective à un environnement numérique ; d'autres personnes, généralement des personnes physiques, profitent de ces éléments pour les détourner de leur identité habituelle et jouir d'un certain niveau d'anonymat.

Beaucoup de personnes physiques créent un avatar qui reflète leur alter ego, mais qui, en ne révélant pas leur véritable identité dés le début, leur permet de naviguer avec plus de liberté dans les médias numériques.

Comme l´écrit Alain Bobant dans la préface du livre intitulé" Internet et les réseaux sociaux", depuis 2005 l'internaute a un comportement sans précédent et adopte la « *Web attitude* » : isolé mais décomplexé, il se montre, se dévoile, s'exprime, s´extériorise, se singularise, se fait remarquer, s´illustre, influence ... Mais en même temps, en interagissant et en s´exhibant, il s´ expose à des risques de toutes sortes.

L'e-réputation est un concept qui a un caractère sociologique mais aussi marketing. Tout au long de notre navigation sur Internet et sur toutes les plateformes sociales qui existent dans ce grand réseau, nous laissons une marque, une marque malheureusement pratiquement indélébile, peut laisser une trace à nos succès professionnels, mais aussi à nos erreurs du passé, des photos peu favorisantes, des amitiés désagréables, etc.

La plus grande difficulté que représente l'e-réputation est qu'elle repose non seulement sur ce que nous pouvons dire ou montrer de nous-mêmes, notre vie ou notre carrière, mais aussi sur des opinions, des photographies, des vidéos et des souvenirs des autres : ces co-habitants du cyberespace qui ne sont pas toujours nos amis ou notre famille, ils sont parfois nos enseignants, nos étudiants, nos collègues, nos clients ou même nos ennemis.

L'importance de l'e-réputation ou de la réputation en ligne est telle qu'il existe aujourd'hui des entreprises qui se consacrent à la vente en ligne de services de nettoyage de réputation.

L'une de ces sociétés est précisément une start-up française appelée SOS réputation, qui propose de "Nettoyer" l'image des personnes ou des entreprises, bien sûr, il ne s'agit pas pas d'effacer un passé négatif mais de "le cacher".

Le contenu des informations auxquelles nous pouvons accéder sur Internet dépendra de la qualité des services fournis par ces fournisseurs (FAI), comme le reconnait la cour d'appel de Paris en 2014. Les FAI peuvent offrir un contenu exclusif et des services innovants exclusifs pour augmentez votre portefeuille de clientèle d'une manière complètement légale.

L'un des grands problèmes de l'activité humaine sur Internet est justement celui des limites presque imperceptibles, grises et ténues : Au nom de la liberté d'expression peut-on dire quoi que ce soit sur Internet ? Quelles sont les règles qui guident notre activité et les normes applicables ?

Grâce aux moteurs de recherche et autres robots, l'identification et la traçabilité des comportements sont consubstantiels aux réseaux numériques. Cette surveillance ne permet en vérité aucune confidentialité des communications. Elle limite l'impunité fréquente de certains comportements dans le monde réel et anéantie même le « droit à l'oubli ». Le résultat est un paradoxe évident : la facilité, la gratuité, l'immédiateté de la communication numérique qui peut engendrer des pratiques individuelles et collectives calomniantes (et parfois condamnable au sens juridique), notamment dans les réseaux sociaux, doivent être mises en perspective avec la facilité d´identifier ces pratiques. Nous faisons face à une banalisation de ce comportement combinée à une augmentation du risque juridique[194].

Tout comme les droits découlent des obligations, la liberté n'est pas absolue, elle a des limites marquées par le bien commun et les droits des tiers. La liberté d'expression née en France avec la révolution, après la proclamation de la Déclaration des droits de l'Homme et du Citoyen de 1789, les articles 10 et 11 prévoientt que d'une part, personne ne devrait être dérangé ou gêné parce qu´il exprime ses opinions, y compris religieuses, à moins qu'elles ne portent atteinte à l'ordre public établi par la loi. D´autre part, la libre communication des opinions et des pensées est l'un des droits les plus précieux de l'homme ; par conséquent, tout citoyen peut parler, écrire et imprimer librement, sauf dans ces cas précis pour lesquels la loi exige que la personne réponde pour abus de cette liberté.

[194] Latreille, Antoine, *Numérisation*, (2017) 22 Lex electronica 117. En : http://www.lex-electronica.org/en/s/1567. Consulté le 9 décembre 2017.

La loi française du 30 septembre 1986 relative à la liberté de communication précise notamment en ce qui concerne l'expression sur Internet, que " L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la protection de l'enfance et de l'adolescence, par la sauvegarde de l'ordre public, par les besoins de la défense nationale.

Pour comprendre ce que l'on entend par "communication publique par voie électronique", aux termes de la loi susmentionnée : " On entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée ".

Ensuite, l'internaute jouit d'une liberté d'expression pleinement reconnue pour pouvoir s'exprimer en ligne, que ce soit sur un blog, un réseau social, un forum de discussion, etc., dans les limites fixées par la loi, et principalement celles liées à dignité, honneur et respect de la vie privée.

Aux États-Unis, la loi présente des différences substantielles. Le premier amendement de la Constitution des États-Unis, adopté en 1791, interdit toutes les restrictions à la liberté religieuse, à la liberté d'expression et à la liberté de la presse.

La Constitution politique des États-Unis Mexicains, dont la tradition est plus attachée à l'esprit de la législation européenne qu'à la tradition américaine, reconnaît également le droit à la liberté d'expression et à la liberté de la presse, dans la limite de l'affectation à des tiers, avec la prescription suivante :

> *"...Article 6. La manifestation des idées ne fera l'objet d'aucune inquisition judiciaire ou administrative, à moins qu´elle ne porte atteinte à la morale, à la vie privée ou aux droits des tiers, occasionne un crime ou trouble l'ordre public ; Le droit de réponse est exercé dans les conditions prévues par la loi. Le droit à l'information sera garanti par l'État*
>
> *Toute personne a le droit d'accéder librement à une information*

pluraliste et opportune, ainsi que de rechercher, recevoir et diffuser des informations et des idées de toute nature par tout moyen d'expression …"

En complément de l´ :

"…Article 7. La liberté de diffuser des opinions, des informations et des idées par tous les moyens est inviolable. Ce droit ne peut pas être restreint par des voies ou moyens indirects, tels que l'abus de contrôles officiels ou privés, la restriction de papier pour l´impression de journaux, les fréquences radio ou les équipements utilisés pour la diffusion de l'information ou par tout autre moyen et technologie de l´ information et communication visant à empêcher la transmission et la circulation d'idées et d'opinions

Aucune loi ou autorité ne peut instituer une censure préalable, ni restreindre la liberté de diffusion, qui n'a pas d'autres limites que celles prévues au premier alinéa de l'article 6o. de cette Constitution. En aucun cas ne pourront être réquisitionné les biens utilisés pour la diffusion d'informations, d'opinions et d'idées en tant qu'instrument de la criminalité.

Dans la réalité, les utilisateurs d'un réseau social tel que Facebook confrontés à la législation applicable par contrat lors d´un litige en Californie, États-Unis, auraient toute liberté de s'exprimer même si cette expression viole certaines limites reconnues par les lois françaises et mexicaines. Cependant, le 5 mars 2015, le tribunal de la Grande Instance de Paris a été jugé compétent pour juger du comportement d'un utilisateur de Facebook. De même, les autorités mexicaines ont le droit de porter l'affaire devant leur juridiction dans les différents domaines de leurs compétences, si un comportement viole les droits du Mexique et lorsqu'elles sont exprimées sur un réseau social établi aux États-Unis.

Il est donc clair que les limites imposées par les droits des tiers et l'ordre public sont applicables à la liberté d'expression indépendamment de la juridiction contractuelle. Tel le prouve le cas de la condamnation imposée à Google par la Haute Cour de Paris le 6 novembre 2013, pour qu´il cesse de publier des photos de la vie sexuelle d'un leader de la course automobile ; ainsi que beaucoup d'autres cas, y compris bien sûr des cas de droit à l'oubli en Europe et au Mexique illustré également par un cas de jurisprudence contre Google.

En plus des risques pour la vie privée liés par l'interaction sur Internet, il est également important d'en souligner d'autres, tels que les crimes contre l'honneur. Malheureusement, ces crimes ont été abrogés graduellement des codes pénaux mexicains depuis 2007. Dans le cas de la France, la loi du 29 juillet 1881 sur la liberté de la presse, précise les règles qui doivent être respectées par tout type de publication, y compris celles faites sur Internet. L´article 29 définit ce ce que l'on entend par diffamation : «Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation. La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, "

Au Mexique et aux États-Unis, des actions civiles sont envisagées pour obtenir réparation en cas de dommages moraux.

La question devient très intéressante face au risque potentiel de voir notre image et notre réputation numérique affectées par un certain type de diffamation à travers un réseau social. Certains réseaux sociaux sont plus enclins à ces situations illicites comme Twitter, Facebook ou Instagram, mais Twitter l´est plus puisque les gens peuvent, sans aucune restriction préalable, affirmer des faits ou des circonstances fausses qui peuvent causer un préjudice moral ou économique à la personne physique ou morale diffamée.

Le 26 juillet 2011, le Tribunal de Commerce de Paris a condamné le dirigeant d'une entreprise à verser 10 000 euros de dommages et intérêts à un prestataire de services pour l´avoir dénigré sur le réseau social Twitter.

Cela dit, la personne accusée de diffamation peut être innocentée si elle prouve de façon concluante que les faits qu'elle affirme sont vrais, tant qu'ils n'impliquent pas de circonstances qui correspondent à la vie privée de la personne concernée.

L'intérêt pour la protection des données personnelles est né à différents moments et dans les trois pays partis de notre enquête.

Dans le cas des États-Unis, dont la législation est beaucoup plus laxiste et permissive et il n'y a pas de loi fédérale ou générale, mais une législation sectorielle isolée et complémentaire. Même si la première référence au droit à la vie privée date de 1890.

Les raisons qui ont donné lieu à la protection de certaines informations d'une manière sectorielle sont dues aux finalités pour lesquelles les informations sont traitées, et n'incluent pas de norme de protection dans tous les domaines de la vie humaine. Par exemple, est en ce qui concerne le commerce et l'économie, les renseignements personnels ont un niveau de protection minimal, tandis que les renseignements médicaux d'une personne bénéficient d'un niveau de protection plus élevé.

Dans certains cas, le système de protection des données personnelles en vigueur aux États-Unis est confus et complexe, car les différents congrès d'État ont établi des recommandations et des paramètres d'autorégulation souvent contradictoires.

Il convient de mentionner qu'une grande partie des efforts qui ont été déployés sont motivés par l'étranger grâce aux accords de libre-échange et aux relations commerciales avec des entreprises de pays dont la réglementation en la matière est beaucoup plus rigide, comme c'est le cas des pays européens.

Ce fut la raison de la mise en œuvre de l'accord Safe Harbour favorisé par l'Union européenne en mai 2000.

L'histoire de la France est diamétralement différente, non seulement par la date à laquelle l'histoire de la protection des données a commencé à être écrite dans ce pays, mais principalement pour la reconnaissance importante du droit à la protection des données personnel comme fondamental dans la vie des citoyens français.

S'il est vrai que le concept de *fichier* personnel n'est pas nouveau et date de plusieurs siècles, en particulier avec l'entrée dans nos vies de dispositifs de traitement de l'information automatisés également connus sous le nom de systèmes informatiques, le traitement de l´information sous forme massive est apparu pour la première fois dans les années 70.

En 1999, le Conseil constitutionnel a accordé sa valeur constitutionnelle en vertu de l'article 2 de la Déclaration des droits de l'homme et du citoyen au droit à la vie privée,

Alors que le respect de la vie privée a été intégré au Code civil français en 1970, son article 9 dispose que " Chacun a droit au respect de la présomption d'innocence. Le juge peut, même en référé, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que l'insertion d'une rectification ou la diffusion d'un communiqué, aux fins de faire cesser l'atteinte à la présomption d'innocence, et ce aux frais de la personne, physique ou morale, responsable de cette atteinte."

Une référence importante pour notre étude a été en outre la lettre de la Cour de Grande Instance de Paris du 13 novembre 2013 où l'étude de l'article 9 du Code Civil est approfondie, déclarant que toute personne a, en vertu du texte précité, le droit exclusif sur sa propre image, attribut de la personnalité, sur l'usage de celle-ci. Ce droit lui permet, en principe, de s'opposer à la diffusion de ces éléments sans son autorisation et d'obtenir réparation du préjudice causé.

Il est important de souligner que le terme « vie privée » est un concept à géométrie variable, qui dépend de divers facteurs de fait et de droit. Par exemple, une personne dont l'activité habituelle ressort de la vie publique, comme certaines actrices ou chanteur célèbre ; ou encore, le cas d'un fonctionnaire qui par loi doit rendre certaines activités de sa vie transparente. C´est pourquoi la définition du concept de "vie privée" pour résoudre un cas spécifique devra prendre en compte certaines circonstances comme par exemple la situation précise de la personne dont la vie intime a été envahi.

Cependant, au-delà de la protection de la vie privée, nous touchons du doigt un domaine de protection précise qu'est la protection des données personnelles.

Il est important de dissocier les domaines de la protection des données personnelles de celui de la vie privée: Simplement parce que toutes les données personnelles ne sont pas de nature privée et que tous les éléments de notre environnement intime ne renvoient pas à des données personnelles.

Comme nous l'avons mentionné précédemment, la naissance des systèmes informatiques et des réseaux de communication mondiaux, en particulier Internet, est venue donner une nouvelle transcendance et nuance à la protection des données personnelles.

La loi française qui réglemente la protection des données personnelles est la Loi

Informatique et les libertés de 1978. Aux termes de l'article 2, Constitue une donnée à caractère personnel « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. " En conséquence de cette même loi, celle créée en 1978 pour l'application de la même loi, était la Commission Nationale des Technologies de l'Information et des Libertés (CNIL), en tant que régulateur des données personnelles des citoyens français.

Le droit européen de protection des données personnelles cherche à équilibrer d'une part la protection de la vie privée et l'innovation et la modernisation de l'économie mondiale, respectant les principes de base de la protection des données personnelles. Le droit français en particulier repose sur le droit à décider de l'utilisation des données personnelles et contrôler cette utilisation, en suivant les principes suivants :

1. Information et consentement
2. Les droits d'accès, de rectification et d'opposition ;
3. Objectif du traitement
4. Qualité
5. Limitation de la période de conservation et
6. Sécurité

En général, le fondement et les principes directeurs de la loi mexicaine sont mentionnés dans les points ci-dessus.

L'histoire de la législation mexicaine en matière de protection des données personnelles a été écrite différemment. Il convient de noter que d'une manière générale, dés les premières réflexions à ce sujet, des lois différentes ont été crées pour les individus et le gouvernement. Indépendamment des initiatives fédérales qui seront analysées plus tard, les premières avancées de manière spécifique étaient isolées. Ces dispositions ont été à peine ébauchées dans la Loi fédérale sur la transparence et l'accès à l'information publique gouvernementale. D´autre part, deux des propositions locales sont applicables aux particuliers, tandis que la troisième proposition de caractère local s'applique aux individus et au gouvernement.

CONCLUSIOS FINALES

- L'identité numérique comprend beaucoup plus d'aspects de ceux qui sont envisagés à première vue : c'est notre empreinte virtuelle authentique, chaque jour nous construisons une histoire et laissons une trace de notre activité dans l'environnement numérique, nos goûts, préférences, peurs, traits de personnalité et en général, tout ce qui nous individualise et fait de nous ce que nous sommes. Cette identité est aujourd'hui plus exposée que jamais, c'est pourquoi nous devons être particulièrement attentifs à tout ce que nous laissons transparaître de notre intimité la plus profonde.

- Ce que nous appelons communément l'usurpation ou le vol d'identité n'est rien de plus que le vol d'identifiants, et en fait, en tenant compte des principes concepts et dogmes fondamentaux du droit criminel, est une nouvelle nuance de fraude

- Le délit d'usurpation d'identité n'est pas un comportement illégal isolé, c'est-à-dire avant ou après il y a eu ou aura d'autres actes illicites. Ce délit ne peut être commis que comme moyen préparatoire d'un autre crime. Nous ne devrions pas étudier ce comportement isolément, mais comme un ensemble en lien avec les faits qui lui ont donné lieu ou lui donneront lieu à l'avenir. L'enquête sur les cas de vol d'identité n'est pas facile, comme nous l'avons décrit, ils peuvent être des cas asymptomatiques dont les conséquences apparaissent longtemps après.

- Les organes législatifs en vigueur dans les trois pays, le Mexique, les États-Unis et la France, sont suffisants nombreux et suffisants pour faire face aux menaces à l'identité numérique. Nous devons faire très attention de ne pas tomber dans le piège de la surrèglementation, en fait il suffit d´une application correcte de la réglementation, une mise en œuvre claire et pertinente des cas, l'obtention et la préservation de preuves numériques appropriées et, enfin, d´une formation correcte aux autorités et aux organes judiciaires pour faire face aux défis qu´imposent ces nouveaux phénomènes de la société de l'information

- Le Mexique possède des laboratoires informatiques à la hauteur des centres d'investigation les plus innovants au monde. Le travail que la division scientifique de la police fédérale a accompli au cours de la dernière décennie, ainsi que celui du bureau du procureur général, et du Secrétariat de la Marine et du Ministère de la Défense devraient être reconnus et mis en évidence, mais avant tout, des efforts devraient être ajoutés pour travailler sur la cybersécurité nationale

- L'étude des cas d´usurpation d'identité ainsi que la stratégie à suivre par les autorités gouvernementales à niveau international pour la combattre, doivent impliquer le travail conjoint de la société civile, du gouvernement et des entreprises et constituer des groupes multidisciplinaires où avocats et experts en technologie réussissent à trouver un terrain commun quand à leur leurs idées et besoins. Toutes les réformes possibles à la législation seront infructueuses si nous ne parvenons pas à comprendre que sous les lois de l'informatique il y a des situations qui échappent parfois au critère classique du juriste.

- La coopération internationale est un élément fondamental de la lutte contre la cybercriminalité, en particulier contre les crimes commis contre notre identité numérique. Il est impératif que le Mexique ratifie la Convention de Budapest et fasse partie de tous les groupes de travail internationaux sur la cybercriminalité, la cybersécurité et le contrôle de l'identité

- Si la cybercriminalité ne connaît pas les frontières internationales elle en respecte moins encore les juridictions étatiques. Ce travail a pour dernière proposition, l'intégration d'un organisme de réglementation fédéral au Mexique. Actuellement, on travaille à la mise en œuvre des accords contenus dans la Stratégie nationale de la cybersécurité en 2017, et ces efforts devraient porter leurs fruits dans les années à venir.