UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

FACULTAD DE DERECHO

TESIS

"LÍMITES JURÍDICOS EN EL USO DE LOS DATOS PERSONALES Y EL RESPETO AL DERECHO DE LA PRIVACIDAD EN UNA ERA DIGITAL"

PRESENTA:

BLANCA ESMERALDA MARTÍNEZ GARCÍA

ASESORA:

DRA. ALEJANDRA FLORES MARTÍNEZ

INTRODUCCIÓN

En la actualidad, la mayoría de las personas en México y en el mundo realiza sus actividades dentro de la red digital o con ayuda de las nuevas tecnologías de la información. Y algunos otros comienzan a incluir con mucho interés el uso de la inteligencia artificial en su día a día, por ello, este trabajo de investigación se dedica a estudiar, analizar y proporcionar las herramientas jurídicas necesarias que se necesitan para comprender y saber defenderse en el entorno en el que actualmente se vive: el digital.

En el campo legal mexicano, el estudio de los datos personales y el derecho a la privacidad en la era digital es un campo que requiere la adecuación de las leyes y concientización de cuidado y protección sobre esta materia en las personas. En este sentido, el presente trabajo de investigación discute la importancia sobre la protección de los datos personales y el derecho a la privacidad en un contexto digital y global.

Dado que esta investigación proporciona un panorama nacional e internacional sobre el uso de los datos personales, se provee de una amplia y enriquecedora fuente de literatura y diversas fuentes del conocimiento que permite la comprensión sobre el uso y cuidado de los datos personales en una era digital. Para ello, se presenta este trabajo en cuatro capítulos. El primer capítulo, hace referencia a todos los conceptos que engloba la protección de datos personales y conceptos afines, los cuales, se pueden encontrar en casi cualquier legislación del mundo.

El segundo capítulo describe algunas situaciones actuales en las cuales se puede usar de manera desfavorable e ilegal los datos personales de las personas en la internet, con la inteligencia artificial, o con las infraestructuras críticas de la información. Así mismo, se facilitan algunas recomendaciones para disfrutar de los múltiples beneficios que también proporciona la era digital y las herramientas tecnológicas, sin tener que ser víctima de algún delito o sufrir algún menoscabo de nuestros derechos humanos.

Ya para el capítulo tres se explica como el “Habeas Data” es el mecanismo por excelencia para ejercer la protección de nuestros datos personales, que, en el caso de México, son los derechos ARCO. Y finalmente el capítulo cuatro se dedica a analizar la legislación mexicana en materia de datos personales, así como proporcionar los mecanismos jurídicos para ejercer los derechos ARCO. En este capítulo también se proporciona algunos precedentes de asuntos relacionados a los datos personales y la privacidad que resolvió la Suprema Corte de Justicia de la Nación.

Capítulo I. Conceptualización de los datos personales y la privacidad

1.1 Delimitación conceptual

Entender la importancia que tiene los datos personales en nuestra vida privada, y sobre todo en la era digital, hace necesario su estudio a profundidad. En este primer capítulo se ofrece una redacción concisa pero exhaustiva de diversos conceptos básicos y afines para entender mejor cómo cuidar y hacer respetar nuestros datos personales.

1.2 Datos personales

a) Doctrina

El uso de los datos personales hoy en día es tan común y cotidiano que en algunas ocasiones se pasa desapercibida la importancia que tiene saber cuidarlos y protegerlos.

Desde el punto de vista doctrinal, para Mendoza “los datos personales refieren a la información del individuo, quien permite identificarlo a través de su descripción, origen, lugar de residencia, trayectoria académica, laboral, entre otros”[1]. Para Meraz, los datos personales “implican cualquier información relacionada con una persona física, sea identificada o identificable, ante la cual existe una obligación de resguardo por parte de sus tenedores y la protección para evitar su divulgación o un mal uso de ella”[2].

[1] Mendoza Enríquez, Olivia Andrea. Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. IUS. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., vol. 12, núm. 41, jan-jun, 2018, pp. 267-291. Consultado el 12 de mayo de 2023. Disponible en: https://www.redalyc.org/pdf/2932/293258387015.pdf

[2] Meraz Espinoza, Ana Isabel. Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales. IUS. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., vol. 12, núm. 41, jan-jun, 2018, pp. 293-310. Consultado el 12 de mayo de 2023. Disponible en: https://www.redalyc.org/pdf/2932/293258387016.pdf

Para Puccinelli, no todos los datos personales requieren una protección jurídica estricta y alude a la distinción que hace Carbó respecto a los distintos grados de protección de los datos personales, la cual es la siguiente:

- "Los datos que son de libre circulación, como los datos de identificación: nombre, apellido, documento de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio.
- Los de circulación restringida a un sector o actividad determinada, que son susceptibles de tratamiento en tanto se presente una causa justificación legítima y con las limitaciones que resulten de esa especialidad.
- Los de recolección prohibida, porque afectan la intimidad personal o familiar, que son los denominados datos sensibles"[3].

b) Legislación nacional

Los datos personales son definidos por los legisladores de manera muy específica y concreta, sobre todo en legislaciones federales, tal es el caso de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que en su artículo 3, fracc. V, define a los datos personales de la siguiente manera: "*V. Datos personales: cualquier información concerniente a una persona física identificada o identificable"*[4]*.*

Por su parte, La Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados, en su artículo 3, fracción IX, proporciona la siguiente definición:

> *"IX. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda*

[3] Cit. Por Mendoza Enríquez, Olivia Andrea. Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. IUS. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., vol. 12, núm. 41, jan-jun, 2018, pp. 267-291. Consultado el 12 de mayo de 2023. Disponible en: https://www.redalyc.org/pdf/2932/293258387015.pdf
También referenciado en Sevilla, D. (2014). El Habeas Data y la protección de Datos Personales en México. [Tesis de licenciatura, Universidad Nacional Autónoma de México].
Repositorio institucional de la Universidad Nacional Autónoma de México.
http://132.248.9.195/ptd2014/octubre/0720248/0720248.pdf

[4] Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Consultado el 26 de octubre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

determinarse directa o indirectamente a través de cualquier información"[5].

c) Legislación internacional

México suscribió diversos tratados y convenios en distintas materias con varios países para la ayuda recíproca en cuanto a derechos y obligaciones se trata, pero en el caso de la legislación internacional en el ámbito del derecho a la protección de los datos personales es muy poca. Se proporciona la siguiente definición establecida en el artículo 2, apartado "a" del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal o también conocido como el Convenio 108: "datos de carácter personal" significa cualquier información relativa a una persona física identificada o identificable ("persona concernida")"[6].

En resumen, los datos personales es toda aquella información relativa a una persona, lo cual la hace identificable. Estos datos personales son importantes porque prácticamente todo lo que acontece a nuestra vida, involucra un dato personal. Luego así, la importancia de conocer cómo cuidarlos y protegerlos ante cualquier posible amenaza es fundamental hoy en día.

Finalmente se menciona que existen otros datos que por su naturaleza los convierten en datos sensibles, información la cual, no sólo hace identificable a una persona, sino que, además, hace que con el uso de esa información sensible se pueda pronosticar la manera de pensar, actuar y decidir de determinada persona. Estos datos son analizados en el siguiente apartado.

---

[5] Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados. Consultado el 17 de octubre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

[6] La entrada en vigor del Convenio 108 en México, fue el 1º de octubre de 2018 y fue publicado en el diario oficial de la Federación el 28 de septiembre de 2018. Consultado el 26 de octubre de 2022. Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5539473&fecha=28/09/2018#gsc.tab=0 También referenciado en López, J. (2018). "El derecho humano al olvido como derecho humano de la era digital". [Tesis de licenciatura, Universidad Nacional Autónoma de México]. Repositorio institucional de la Universidad Nacional Autónoma de México. http://132.248.9.195/ptd2019/marzo/0786916/0786916.pdf

1.3 Datos sensibles

En la esfera de los datos personales, existen los datos sensibles que necesitan una protección legal más amplia. Con el avance de la tecnología, los datos se usan a gran escala y sin una regulación específica, al menos en México. Además, el gran avance de la tecnología hace que incluso sin llegar a solicitar u obtener directamente datos sensibles, los sistemas informáticos obtienen predeterminadamente esos datos sensibles. La importancia de entender y proteger los datos sensibles radica en que estos permiten identificar a una persona en lo más íntimo y, con un uso desmesurado por un tercero, sean Estado o un particular, se puede llegar a controlar sus hábitos, decisiones y pensamientos.

Es importante empezar por definir qué son los datos sensibles, al respecto, Pfeiffer proporciona el siguiente concepto: “son todos aquellos que identifican o permiten la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, de salud, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias puede llegar a constituir una amenaza para el individuo”[7].

Pfeiffer menciona además que “el que recibe los datos sensibles tiene el deber de ser confiable ya que el sujeto que entrega los datos lo hace con carácter “confidencial”, entrega lo que hasta ese momento guardaba para sí de una forma muy especial. Lo da a conocer a la o las personas con quien o quienes comparte “una fe”, con quienes actúa en confianza y que, por ello, le deben confidencialidad”[8]. Trasladado a una esfera más limitada, el titular de los datos personales sabe con exactitud quién es la persona responsable de sus datos personales y sensibles, como puede ser el caso de un abogado, una médica, un sacerdote, una psicóloga,

[7] Pfeiffer, M. 2008. Derecho a la privacidad. Protección de los datos sensibles. Revista Colombiana de Bioética, vol. 3, núm. 1, enero-junio, 2008, pp. 11-36. Consultado el 13 de febrero de 2023. Disponible en: https://www.redalyc.org/articulo.oa?id=189217248002
En el mismo sentido está en Medina, M. (2020). Los datos personales análisis jurídicos desde la perspectiva del funcionalismo. [Tesis doctoral, Universidad Nacional Autónoma de México]. Repositorio institucional de la Universidad Nacional Autónoma de México.
http://132.248.9.195/ptd2020/septiembre/0803167/Index.html
[8] *Íbidem*.

entre otros, y hasta cierto punto se exige una responsabilidad directa al responsable del tratamiento. El problema comienza a surgir cuando de manera indirecta y sin saber quién es el responsable directo de nuestros datos los comienza a usar sin la voluntad del titular de dichos datos.

La ley mexicana, a través de la LFPDPPP en a su artículo 3, fracción VI, define a los datos sensibles de la siguiente manera:

> *"Datos personales sensibles: "aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual"[9].*

Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 3, fracción IX, hace una ligera distinción al concepto, al mencionar algunos ejemplos sobre los datos personales sensibles de manera enunciativa, más no limitativa. Se proporciona la siguiente definición para mayor ilustración:

> *"Datos personales sensibles: "aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética,*

[9] Ley Federal de Protección de Datos Personales en Posesión de Particulares. Consultado el 08 de noviembre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual"[10].

De esta manera, se alcanza a distinguir la importancia que conlleva un adecuado manejo no solo de los datos personales, sino también de los datos personales sensibles, porque estos implican un mayor alcance a la vida privada y a la intimidad de las personas (conceptos que se abordarán en los siguientes apartados), derechos que, junto con otros muy diversos, el mal uso podría afectar directamente cualquier aspecto de la vida personal del titular de los datos. De ahí la importancia no sólo de entender qué son estos datos sensibles y qué leyes los protegen, además, comprender el poder que tienen los datos, los cuales son muy codiciados por empresas y gobiernos.

1.4 Derecho a la protección de los datos personales

Debido a que los datos personales y los datos sensibles son conceptos que cada vez están presentes en el día a día, es necesario entenderlos y protegerlos ante cualquier tipo de amenaza, de ahí que exista el derecho a la protección de los datos personales.

Un interesante concepto de este derecho es definido por Quijano como "derecho fundamental que faculta a la persona a decidir qué información concerniente a ella proporciona a un tercero, saber quién dispone de esa información y para qué, y oponerse a esa posesión o uso por parte de otras personas"[11]. A diferencia de otros autores, Quijano proporciona un concepto de derecho a la protección de datos personas de manera general. Por otra parte, Seoane proporciona un concepto más acorde la realidad actual, y define este derecho como "conjunto de facultades que le permiten a la persona tener control sobre el tratamiento de sus propios datos, bien sea que estos se encuentren en soportes manuales o automatizados o que

[10] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 08 de noviembre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[11] Quijano Decanini, Carmen. Derecho a la privacidad en Internet. 2022. México. Tirant lo Blanch. Consultado el 11 de noviembre de 2023.

hagan referencia a su vida íntima o privada, e imponer a terceros que actúen o se abstengan de realizar acciones respecto de ellos”[12].

En la legislación mexicana no ofrece concepto concreto alguno referente a este derecho, aun así, los parámetros generales para proteger este derecho se logran a través de principios establecidos en las respectivas leyes de la materia, y con la aplicación de los derechos ARCO (derechos de acceso, rectificación, confirmación, y oposición), los cuales se analizarán en el apartado correspondiente de este capítulo.

El derecho de protección de datos personales esta intrínsecamente relacionado con el derecho al honor, el derecho a la propia imagen, el derecho a la intimidad, a la privacidad, a la vida privada y a la autodeterminación informativa (conceptos que son analizados a lo largo de este capítulo). La importancia de su regulación en el uso de datos personales es porque faculta al titular el determinar cómo se hará el acceso y tratamiento de sus datos personales, así mismo en la rectificación, cancelación u oposición.

1.5 Vida privada y derecho a la privacidad

La privacidad es un concepto difícil de establecer. No se observa en la doctrina ni en la jurisprudencia una delimitación conceptual precisa y unívoca de este derecho. Además de que es un concepto que evoluciona a lo largo de los años.

Hay muchas definiciones, teorías e interpretaciones sobre la privacidad, por lo que es casi imposible que los jueces, abogados e investigadores coincidan en una definición común, puesto que se trata de un concepto que históricamente cambió su significado según el contexto social.

[12] Cit. Por Gómez-Córdoba, Ana, Arévalo-Leal, Sinay, Bernal-Camargo, Diana, & Rosero de los Ríos, Daniela. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Revista de Bioética y Derecho*, (50), 271-294. Epub 23 de noviembre de 2020. Recuperado en 11 de noviembre de 2022. Disponible en: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300017&lng=es&tlng=es.

Sin embargo, este trabajo de investigación proporciona la siguiente definición que, de acuerdo con Santos Cifuentes “la privacidad es un valor fundamental de la persona, un aspecto constitutivo de su propio ser. La construcción y desarrollo de la personalidad psicológica solo es posible si el individuo puede mantener por decisión propia un conjunto de aspectos, circunstancias, y situaciones a no ser compartidas con el mundo exterior”[13]. Santos Cifuentes también menciona que:

> *“Lo que comúnmente se reconoce como privacidad en las sociedades respetuosas de derechos humanos, estriba en que le corresponde al individuo a decidir acerca de la creación, cuidado y uso de sus pensamientos y de su información, como asuntos propios reservados de la injerencia de terceros, elegir sus relaciones, mantenerlas, y acabarlas sin intromisión de nadie y decidir cuáles son las conductas confidenciales de su vida individual. Si esto no fuera posible se colocaría al ser humano en estado de dependencia, de indefensión, pues quedaría sometido a la exterioridad, que lo exhibe y lo deshumaniza”[14].*

Debido a que las circunstancias económicas, sociales, políticas, culturales y sobre todo las tecnológicas cambiaron con el paso de los años, el concepto de privacidad cambió conjuntamente. A pesar de ello, Solove clasificó las distintas acepciones que la doctrina dio a este derecho, y son las siguientes: “1. El derecho a ser dejado solo, 2. El ámbito de acceso limitado a uno mismo, 3. La facultad de secrecía o de ocultar ciertos asuntos, 4. El control de la información personal, 5. La protección de la personalidad, individualidad y la dignidad, y 6. El derecho a la intimidad o el control sobre las relaciones íntimas o sobre ciertos aspectos de la vida”[15].

Una de las preocupaciones más recientes sobre este ámbito, estriba en que hoy en día casi todo está conectado a la internet, con lo cual, los responsables de recabar,

[13] Cit. Por Quijano Decanini, Carmen. Derecho a la privacidad en Internet. 2022. México. Tirant lo Blanch. Pág. 54. Consultado el 11 de noviembre de 2023.
[14] *Ibidem*, pág. 55.
[15] Cit. Por Quijano Decanini, Carmen. Derecho a la privacidad en Internet. 2022. México. Tirant lo Blanch. Pág. 55 Consultado el 11 de noviembre de 2023.

almacenar y tratar datos personales tienen una gran responsabilidad con los titulares para que sus datos sean tratados y analizados sin interferir en su vida privada y sin vulnerar sus derechos humanos.

Crece exponencialmente la preocupación sobre la vigilancia masiva en internet, el monitoreo constante en las ciudades, la creación de perfiles en internet con base en datos que son obtenidos por el uso de una red social, una aplicación o algún servicio. Es necesario que la sociedad en general conozca sobre el tema para así evitar interferencias en su vida privada.

Por su parte, el derecho mexicano regula el derecho a la vida privacidad y a la protección de los datos personales se encuentra regulada en la Constitución Política de los Estados Unidos Mexicanos de la siguiente manera:

> "*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 […]"*[16].

La constitución mexicana regula a la vida privada de diversas maneras, tanto en cuanto a posesiones, derechos, deberes y obligaciones, sin embargo, esta investigación hará énfasis a la protección de los datos personales.

> "*Artículo 16*. […]
>
> *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,*

[16] Constitución Política de los Estados Unidos Mexicanos. Consultado el 26 de octubre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

seguridad y salud públicas o para proteger los derechos de terceros"[17].

Por su parte, el Pacto Internacional de Derechos Civiles y Políticos (ONU), dispone:

"Artículo 17.

1. *Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o reputación*"[18].

1.6 Otros conceptos afines

a) Derecho a la imagen

Hoy en día, resulta indispensable para casi cualquier persona tener a la mano el uso de un teléfono inteligente. Se le llama inteligente porque con él una persona puede hacer casi cualquier actividad, desde consultar el estado del tiempo, ver las noticias, tomar fotografías, ver una película, hacer compras, realizar pagos bancarios, mandar mensajes, difundir mensajes, reservar en un restaurante entre muchas más actividades. Debido al gran impacto de las fotografías, las imágenes y vídeos, su uso tanto en medios tradicionales como en medios modernos de comunicación son cada vez más valiosos. Una imagen, una palabra o un buen vídeo puede influir directa o indirectamente en una persona. Ahora, es más fácil captar la imagen o movimientos de las personas con ayuda de los teléfonos inteligentes. Esta actividad se convirtió tan cotidiana en nuestros días que muchas veces la gente no conoce la importancia que tiene el proteger la imagen de las personas. Y en muchas

[17] *Idem*.
[18] Estrada Avilés, Jorge Carlos. EL DERECHO A LA INTIMIDAD Y SU NECESARIA INCLUSION COMO GARANTIA INDIVIDUAL. Consultado el 26 de octubre de 2022. Disponible en: http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf
También referenciado en Eguiguren, F. (2004). "Libertades de expresión e información, intimidad personal y autodeterminación informativa: contenido, alcances y conflictos". [Tesis de maestría, Pontificia Universidad Católica de Perú]. Repositorio institucional de la Pontificia Universidad Católica de Perú.
https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/4750/EGUIGUREN_PRAELI_FRANCISCO_LIBERTADES_EXPRESION.pdf?sequence=7&isAllowed=y

ocasiones, estas imágenes, fotografías o vídeos se obtuvieron sin el consentimiento de las personas.

Proteger el derecho a la imagen implica una serie de desafíos, ya que como se expuso, la obtención de imágenes de personas se convirtió en una actividad muy fácil y accesible de hacer hoy en día, para lo cual y de acuerdo con Risso, esta acción trajo consigo dos fenómenos: “a) la importancia de la imagen (hoy lo es todo, es lo que atrae, lo que vende y lo que interesa) y la facilidad con la que se puede acceder a imágenes de calidad respecto a casi todo, y b) la rapidez con que cambia lo que interesa (lo que importa hoy no tiene la más mínima trascendencia mañana)”[19].

Para entender mejor el tema, Flores define a la imagen como “la representación gráfica de la figura humana y el derecho a la propia imagen es a facultad para permitir o impedir su obtención, reproducción y/o difusión por parte de un tercero, así como para obtener beneficios económicos por la explotación comercial de la misma”[20]. En este sentido, Risso resalta la importancia de la propia imagen y que su protección es mayor que en el pasado. El grado de exposición de la imagen de un individuo, la facilidad para captarla y el alcance que tiene hoy su difusión, son enormes. Y no se olvide la tendencia creciente de muchas personas a exhibir su propia imagen en las redes y transmitir imágenes propias y de otros[21].

La importancia del derecho a la propia imagen cobró mucha importancia en esta época, ya que debido al rápido acceso de las cámaras fotográficas y a las videocámaras, se volvió más fácil difundir imágenes y vídeos por casi todo el mundo, sin embargo, podemos encontrar casos en los que el derecho a la propia imagen se vulneró junto con otros derechos más. Tal es el caso de la STS del 15

[19] Risso Ferrand, Martin. Derecho a la propia imagen y expectativa de respeto a la privacidad. Centro de Estudios Constitucionales de Chile Universidad de Talca. ISSN: 0718 0195. Consultado el: 29 de septiembre de 2022. Disponible en: https://pdfs.semanticscholar.org/eb5e/5a565ddb36918c412c0e29dc0a435977a537.pdf

[20] Cit. Por Quijano Decanini, Carmen. *Derecho a la privacidad en internet.* México. 2022. Colección Tirant 4.0., pág. 59.

[21] Risso Ferrand, Martin. Derecho a la propia imagen y expectativa de respeto a la privacidad. Centro de Estudios Constitucionales de Chile Universidad de Talca. ISSN: 0718 0195. Consultado el: 29 de septiembre de 2022. Disponible en: https://pdfs.semanticscholar.org/eb5e/5a565ddb36918c412c0e29dc0a435977a537.pdf

de diciembre de 1998 dictada en relación a dos africanos padre e hijo nacionalizados españoles que ejercían el comercio en el Rastro madrileño con licencia, permisos y pago de los impuestos correspondientes y en un reportaje periodístico se decía al pie de los efigiados:

> *"Estos dos africanos ilegales montan un tenderete en el Rastro Madrileño. El hecho es que en la mayoría de los casos cuando se vulnera la privacidad, la fama y el honor personal al publicarse una imagen, se dañan en primera instancia el respeto a la imagen personal, por ser su representación física parte indivisible de ella, y se suman a ello, los daños ocasionados al honor, fama o privacidad*[22]*.*

Es muy interesante analizar este caso bajo las leyes mexicanas, ya que, desde el punto de vista jurídico, la Ley de Derechos de Autor permite a los fotógrafos profesionales exhibir las fotografías realizadas bajo el encargo como muestra de su trabajo, previa autorización del sujeto, pero esto no será necesario cuando se trate de fines culturales, educativos o de publicaciones sin fines de lucro, esto de acuerdo con su artículo 86. Por su parte el artículo 87 de la misma Ley estipula "*que el retrato de una persona sólo puede ser usado o publicado, con su consentimiento expreso, o bien con el de sus representantes o los titulares de los derechos correspondientes, pero este no será necesario cuando se trate del retrato de una persona que forme parte menor de un conjunto o la fotografía sea tomada en un lugar público y con fines informativos o periodísticos*"[23], permitiendo así a los fotógrafos capturar imágenes de cualquier persona sin saber si daña su honor, reputación, su imagen personal o hasta su vida privada. Además, otro punto controversial de los artículos en cuestión es que hoy en día es complicado determinar con precisión lo relativo a "fines informativos", que hoy lo es casi todo.

[22] Flores Ávalos, Elvia Lucía. Derecho a la imagen y responsabilidad civil. Consultado el 1 de noviembre de 2022. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/4/1943/21.pdf
[23] Ley Federal de Derechos de Autor. Consultado el 01 de noviembre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/122_010720.pdf

b) Derecho al honor

El honor es un concepto que es usado desde hace muchos años. Al igual que el concepto de privacidad, éste evolucionó con el paso de los años. El honor es un concepto que se ve influenciado por muchas circunstancias. Al respecto, Merino argumenta que “es necesario y pertinente hacer una distinción entre personas físicas y morales para saber cómo le asiste el derecho al honor”[24]. También menciona que "el derecho al honor es un derecho de la personalidad que se distingue por dos elementos: uno subjetivo, que corresponde a la esfera íntima de las personas, es decir, cómo se valoran y se ven a sí mismas en relación con la sociedad; y uno objetivo, que se refiere a la consideración que las demás personas tienen de uno mismo”[25].

El derecho al honor es entonces, un derecho de personalidad sin el cual no puede ser una persona. Este derecho implica lograr una armonía entre lo que el sujeto piensa sobre sí y lo que la sociedad piensa sobre él o ella. Dependiendo de las circunstancias sociales, culturales, políticas, éticas, morales e incluso económicas, este derecho al honor sufre algunas variaciones en cuánto a su interpretación. Generalmente engloba dentro de su núcleo protector el derecho al buen nombre, a la propia estima, a la dignidad personal, a la reputación y a la buena fama[26].

Hoy en día, y debido al gran poder que tienen los medios de comunicación tradicionales y modernos, el juicio y la opinión de la gente se ve, en la mayoría de las veces, directamente influenciada por lo que se lee, ve y escucha en estos medios de comunicación masiva. Muchas veces el honor se va formando a través de un constructo social en el que intervienen distintos y variados factores.

En México, la Constitución Política de los Estados Unidos Mexicanos no proporciona alguna garantía judicial específica que regule este derecho, sin embargo, la SCJN

---

[24] Merino, L. Libertad de expresión y derecho al honor: colisión de dos derechos entre medios de comunicación. Instituto de Investigaciones Jurídicas de la UNAM. Consulta el 14 de febrero de 2023. Disponible en: https://revistas-colaboracion.juridicas.unam.mx/index.php/decoin/article/viewFile/33236/30200

[25] *Ibidem.*

[26] Quijano Decanini, Carmen. *Derecho a la privacidad en internet.* México. 2022. Colección Tirant 4.0., pág. 61

para salvaguardar el derecho al honor, publicó una tesis de jurisprudencia sobre el derecho fundamental al honor:

> **DERECHO FUNDAMENTAL AL HONOR. SU DIMENSIÓN SUBJETIVA Y OBJETIVA[27].**
>
> A juicio de esta Primera Sala de la Suprema Corte de Justicia de la Nación, es posible definir al honor como el concepto que la persona tiene de sí misma o que los demás se han formado de ella, en virtud de su proceder o de la expresión de su calidad ética y social. Todo individuo, al vivir en sociedad, tiene el derecho de ser respetado y considerado y, correlativamente, tiene la obligación de respetar a aquellos que lo rodean. En el campo jurídico esta necesidad se traduce en un derecho que involucra la facultad que tiene cada individuo de pedir que se le trate en forma decorosa y la obligación de los demás de responder a este tratamiento. Por lo general, existen dos formas de sentir y entender el honor: a) en el aspecto subjetivo o ético, el honor se basa en un sentimiento íntimo que se exterioriza por la afirmación que la persona hace de su propia dignidad; y b) en el aspecto objetivo, externo o social, como la estimación interpersonal que la persona tiene por sus cualidades morales y profesionales dentro de la comunidad. En el aspecto subjetivo, el honor es lesionado por todo aquello que lastima el sentimiento de la propia dignidad. En el aspecto objetivo, el honor es lesionado por todo aquello que afecta a la reputación que la persona merece, es decir, el derecho a que otros no condicionen negativamente la opinión que los demás hayan de formarse de nosotros.

Es esencial comprender y distinguir estos derechos, ya que su importancia radica en saber qué esfera de la vida de la persona se está afectado: la privada o la pública. Cuando hablamos del ámbito del internet pueden existir intromisiones ilegítimas al derecho al honor que no impliquen una violación a la privacidad. Por ejemplo, cuando se usan expresiones o mensajes con el propósito de provocar el desprestigio de una persona, de sus amigos o de sus familiares y éstas se difunden

[27] Tesis 118/2013. Semanario Judicial de la Federación y su Gaceta, Décima época, Libro 3, Tomo I, febrero de 2014. Consultado el 03 de octubre de 2022. Disponible en: https://sjf.scjn.gob.mx/SJFSem/Paginas/Reportes/ReporteDE.aspx?idius=2005523&Tipo=1

por internet, aunque el contenido de esos mensajes no se obtenga de información reservada sino de información conocida legítimamente o cuando se desprestigia a un individuo sin necesidad de usar datos muy concretos o información personal del mismo. En estos casos no existe una violación a la privacidad, pero sí una violación al honor, porque basta con el agravio intencionado a la estimación propia o ajena a la persona[28].

c) Derecho a la intimidad

Es difícil hablar de intimidad cuando casi todo lo que ocurre en nuestras vidas es mostrado en redes sociales. Es aún más complicado cuando las empresas dedicadas al tratamiento de datos personales vulneran nuestra privacidad al crear perfiles de usuarios en los cuales pueden obtener datos específicos de nuestra vida.

Debido a que el interés y la comercialización (y la banalización) de la vida privada de las personas es un fenómeno que ha ido en aumento, el derecho a la intimidad se ve vulnerado por el uso del internet, en especial por el uso de redes sociales por parte de las generaciones más jóvenes. En un principio no se distinguía con precisión el derecho a la propia imagen del derecho al honor y a la intimidad. En muchos pronunciamientos judiciales se descartaba la vulneración del derecho a la propia imagen cuando no se advertía lesión del honor o la intimidad[29]. A pesar de que no existe un consenso jurídico doctrinal y mucho menos legal, se hace referencia a lo que diversos autores estudiaron acerca del concepto intimidad. Zavala de González considera que la intimidad es "el derecho personalísimo que protege la reserva espiritual de la vida privada del hombre, asegurando el libre desenvolvimiento de éste en lo personal, en sus expresiones y en sus afectos"[30].

---

[28] Quijano Decanini, Carmen. *Derecho a la privacidad en internet.* México. 2022. Colección Tirant 4.0., pág. 63.

[29] Risso Ferrand, Martin. Derecho a la propia imagen y expectativa de respeto a la privacidad. Centro de Estudios Constitucionales de Chile Universidad de Talca. ISSN: 0718 0195. Consultado el: 29 de septiembre de 2022. Disponible en: https://pdfs.semanticscholar.org/eb5e/5a565ddb36918c412c0e29dc0a435977a537.pdf

[30] Cit. Por Cobos Campos, Amalia Patricia. (2013). El contenido del derecho a la intimidad. *Cuestiones constitucionales*, (29), 45-81. Recuperado en 03 de noviembre de 2022, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-91932013000200003&lng=es&tlng=es.

Por su parte, Vásquez considera que “la intimidad es el conjunto de sentimientos, pensamientos e inclinaciones más internos —la ideología, la religión o las creencias—, las tendencias personales que afectan a la vida sexual, determinados problemas de salud que deseamos mantener en total secreto, u otras inclinaciones [...]”[31].

Dado que en nuestro país no existe una regulación expresa sobre el derecho a la intimidad, sí lo existe implícitamente en diversos artículos constitucionales, de leyes secundarias y tratados internacionales. Un ejemplo es el artículo 6º constitucional de México que en menciona:

> “*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”*[32].

En este precepto constitucional se vislumbra la garantía judicial que se le da al derecho a la privacidad y, aunque como se mencionó anteriormente, no es en sí ni siquiera un sinónimo del derecho a la intimidad, este derecho a la vida privada sí protege implícitamente el derecho a la intimidad como un elemento de este.

Lo mismo ocurre con la Declaración Universal de los Derechos Humanos, que a pesar de establecer en su artículo número 12 la no injerencia a la vida privada, al ataque a su honra o su reputación, no se menciona explícitamente la tutela al derecho a la intimidad.

---

[31] *Idem.*
También referenciado en Sevilla, D. (2014). El Habeas Data y la protección de Datos Personales en México. [Tesis de licenciatura, Universidad Nacional Autónoma de México]. Repositorio institucional de la Universidad Nacional Autónoma de México.
http://132.248.9.195/ptd2014/octubre/0720248/0720248.pdf

[32] Constitución Política de los Estados Unidos Mexicanos. Consultado el 03 de noviembre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

> *"Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"*[33].

Fuera de México, se encontraron interesantes conceptos sobre el derecho a la intimidad, tal es el caso de Colombia, que a través de su Corte Constitucional, se analizan los siguientes conceptos: por medio de la sentencia T-787 de 2004, la Corte Constitucional de Colombia define el derecho a la intimidad como la existencia y goce de una órbita reservada de cada persona, exenta del poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad, que le permita a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural[34].

La misma corte menciona ahora en su sentencia SU-056 del 16 de febrero de 1995 que el derecho a la intimidad se refiere a aquellos fenómenos, comportamientos, datos y situaciones que normalmente están sustraídos a la injerencia o al conocimiento de extraños[35]. Por consiguiente, el derecho a la intimidad se refiere a aspectos que abarcan las condiciones de salud, las preferencias sexuales, la ideología política, y cualquier tipo de pensamiento o comportamiento de una persona.

Si bien tampoco existe una regulación específica para el ejercicio del derecho a la intimidad en México, éste es protegido de manera intrínseca por el derecho a la privacidad y en especial por el derecho de protección de datos personales, a través de los derechos ARCO en el caso de México. Es así como el Habeas Data (el cual se analiza a profundidad en el capítulo III) que garantiza, al menos, la mayoría de los derechos que se estudian en este capítulo.

---

[33] Declaración Universal de los Derechos Humanos. Consultado el 03 de noviembre de 2022. Disponible en: https://www.un.org/es/about-us/universal-declaration-of-human-rights

[34] Cit. Por Romero Pérez, X. 2008. El alcance del derecho a la intimidad en la sociedad actual. Revista de Derecho del Estado. Bogotá, Colombia. Consultado el 14 de febrero de 2023.

[35] *Ibidem.*

1.7 Autodeterminación informativa

El derecho de autodeterminación informativa es un concepto nuevo, el cual surge a partir de la necesidad de que sea el titular quien decidida quién, cuándo, cómo y con qué fin serán usados y tratados sus datos personales. Además, este concepto brinda una de las bases necesarias para ejercer el Habeas Data o los derechos ARCO en el caso de México.

Por lo tanto, es importante definir qué es la autodeterminación informativa. En este orden de ideas, Bazán argumenta que:

> *"la autodeterminación informativa consiste en la posibilidad que tiene el titular de los datos personales de controlar quiénes serán destinatarios de éstos y qué uso les darán, y se ejercita genéricamente a través de los derechos de acceso, rectificación y cancelación. Además, ofrece una textura que resulta acorde con los modernos desafíos informáticos, puesto que, abandonando el concepto de intimidad como libertad negativa, permite avanzar hacia una fase activa del proceso de circulación de la información personal brindando protagonismo al interesado al posibilitarle el ejercicio de un adecuado control sobre la misma"*[36].

Con este derecho se pretende que la persona tenga el papel principal para establecer el almacenamiento, tratamiento y uso de sus propios datos personales los cuales, con la era digital, no sólo se hace más fácil la obtención de estos, sino que además actualmente no se reconoce por una gran parte de la población la importancia que tiene saber cómo es que las personas, empresas e incluso el Estado almacenan nuestros datos.

[36] Bazán, V., (2005). El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. Estudios Constitucionales, 3(2),85-139. [fecha de Consulta 20 de noviembre de 2022]. ISSN: 0718-0195. Recuperado de: https://www.redalyc.org/articulo.oa?id=82030204
También referenciado en Pérez, M. 2020. Protección de datos personales y derecho a la autodeterminación informativa: Régimen jurídico. Revista de Derecho No. 28/2020. Consultado el 30 de mayo de 2023. Disponible en: https://doi.org/10.5377/derecho.v0i28.10146

Por su parte, Carmen Quijano señala que “este nuevo concepto comprende la facultad de la persona para conocer, acceder y controlar la información que le concierne. Este derecho a la autodeterminación informativa supone que la persona pueda elegir qué información de su esfera privada es susceptible de ser compartida y cuál no, así como la facultad de decidir quién y en qué condiciones la usa”[37].

En conclusión, se puede establecer que este derecho de autodeterminación informativa, junto con otros, es de vital importancia en una era digital, además su estudio y regulación en las leyes de México y en todos los países del mundo es muy necesario, dado que cada día aumenta el número de usuarios en plataformas digitales, redes sociales y en general, en el uso del internet.

Teniendo en cuenta la existencia de este derecho, es necesario mencionar las garantías que se deben de aplicar para ejercitar este derecho de autodeterminación informativa. Los derechos ARCO (acceso, rectificación, cancelación y oposición), son mecanismos jurídicos clave para ejercer nuestro protagonismo en un mundo digitalizado. Es aquí cuando se hace necesario redoblar esfuerzos tanto por la academia como por el sector público y privado, sobre todo el público, para hacer que la población conozca que no simplemente su vida en la digitalización es estática y sin protagonismo, al contrario, que comprenda que sus datos ingresados en la red, son totalmente suyos, y aunque el gobierno, empresas, instituciones o incluso personas, accedan a sus datos y les den tratamiento, son los mismos titulares de dichos datos lo que deben decidir cómo sus datos serán recopilados, tratados o almacenados.

En el capítulo IV se muestra de manera más específica el cómo ejercitar los derechos ARCO y los mecanismos jurisdiccionales para ejercer nuestros derechos digitales.

[37] Quijano Decanini, Carmen. *Derecho a la privacidad en internet.* México. 2022. Colección Tirant 4.0., pág. 69.

1.8 Derecho informático

El rápido desarrollo de las nuevas tecnologías de la información hace que la sociedad busque nuevas maneras de comportarse y de convivir, y al involucrarse la sociedad en la era digital, se hace necesario el estudio de la relación hombre-internet, creando así el derecho informático.

De esta manera, se creó un nuevo campo en los estudios y práctica jurídica denominado derecho de Internet, derecho del ciberespacio, derecho informático o derecho de las tecnologías de la información; sin embargo, autores reconocidos prefieren referirse a "derecho de Internet" (*Internet law*) antes que a derecho del ciberespacio (*cyberspace law*) o derecho de las tecnologías de la información (*information technology law*), debido a su especificidad y definido ámbito de aplicación. Incluso, el profesor Arno Lodder de la Universidad Libre de Ámsterdam, estableció los "Diez Mandamientos" del derecho de Internet, para los abogados que se ocupan de estos asuntos[38].

Por su parte, el profesor Suñe, afirma que "el derecho de la informática, por seguir aportando razones singulares que avalan su autonomía, tiene mucho de Derecho Global, al tratarse de un Derecho muy internacionalizado, probablemente por el tipo de comunidades humanas que están en su base. La regulación jurídica de Internet, por ejemplo, plantea problemas globales, que requieren soluciones globales. Las grandes multinacionales del sector teleinformático, que lo dominan casi todo por completo, no pueden –ni quieren– adaptarse a regulaciones estatales injustificadamente diversas y dispersas, cuando el mercado no es nacional, sino global"[39]. Al respecto, advierte que son temas propios del Derecho Informático: a) Contratación Informática; b) Derecho a la intimidad y libertades; c). Flujo

[38] Cit. Por Jiménez, W. G., & Meneses Quintana, O. (2017). DERECHO E INTERNET: INTRODUCCIÓN A UN CAMPO EMERGENTE PARA LA INVESTIGACIÓN Y PRÁCTICA JURÍDICAS. Prolegómenos. Derechos y Valores, XX (40),43-61. [fecha de Consulta 30 de noviembre de 2022]. ISSN: 0121-182X. Recuperado de: https://www.redalyc.org/articulo.oa?id=87652654004

[39] Cit. por Velasco Melo, A. H. (2008). El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. Revista de Derecho, (29),333-366. [fecha de Consulta 30 de noviembre de 2022]. ISSN: 0121-8697. Recuperado de: https://www.redalyc.org/articulo.oa?id=85102913

transnacional de datos; d). Propiedad Intelectual del software; y e) Otros temas del Derecho Informático (delitos penales, valor probatorio de los soportes informáticos, transmisión de datos)[40]. Por otro lado, Julio Téllez afirma que el derecho de la informática "es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática"[41].

Desde mi perspectiva, el derecho informático es un conjunto de normas, principios, leyes y jurisprudencia que tiene por objeto de estudio a la informática, y todas sus vertientes que se relacionan con ella. Además el derecho informático es aquella rama del derecho que trabaja interdisciplinariamente con otras ramas del derecho, como el derecho internacional (al analizar qué juez de distintos países resolverá el asunto, así como determinar la ley a obedecer, y el establecer cómo se ejecutará la sentencia), el derecho penal (al encuadrar nuevos delitos penales), el derecho civil (principalmente en contratos), derecho comercial (debido a que el comercio digital crece cada día más), el derecho constitucional (y su principal relación con el derecho de protección de datos personales y la privacidad) entre otras materias.

El estudio del derecho informático se hace cada vez obligatoria en los profesionales del derecho, sin embargo, el conocimiento sobre protección de datos personales y los derechos digitales por parte de la sociedad en general es esencial, ya que es la sociedad la que navegan todos los días en la internet. Además, el elemento principal del derecho de la informática es proporcionar bases jurídicas para evitar cualquier situación que afecte los derechos humanos de las personas en esta creciente era digital.

[40] *Ibidem.*

[41] Cit. Por Ríos Estavillo, Juan José (1997) Derecho e informática en México: informática jurídica y derecho de la informática/ México: Universidad Nacional Autónoma de México. Consultado el 30 de noviembre de 2022. Disponible en: http://ru.juridicas.unam.mx/xmlui/handle/123456789/9121
También referenciado en Medina, M. (2020). Los datos personales análisis jurídico desde la perspectiva del funcionalismo. [Tesis doctoral, Universidad Nacional Autónoma de México]. Repositorio institucional de la Universidad Nacional Autónoma de México. http://132.248.9.195/ptd2020/septiembre/0803167/Index.html

1.9 Neutralidad de la red

En el siglo XX el concepto de neutralidad de la red no existía, y es que, a pesar de que con la tercera revolución industrial (la automatización, el crecimiento de las tecnologías de la información y la comunicación) las tecnologías y las herramientas digitales experimentaban un mayor desarrollo, con ello, surgió la necesidad de mejorar y sacar provecho económico y político a esos mismos sistemas. Fue así, como surge la cuarta revolución industrial, que involucra ahora el internet de las cosas, el cómputo de la nube, los sistemas ciberfísicos y la robótica.

Ya en el siglo XXI se extendió el consumo de internet en los hogares, proceso que se vio favorecido por el desarrollo de la banda ancha, no obstante, no podemos ignorar los diferentes niveles de conectividad de acuerdo con el área geográfica y regional[42].

De acuerdo con Wu, “el concepto de neutralidad de la red (NN) refiere a que los flujos de bits que circulan por internet no deben discriminarse (favorecidos o recortados) por los actores intervinientes”[43], en parte asegurando el espíritu de apertura y colaboración que Berners Lee y Caileau le imprimieron a la Web al liberar y hacer de código abierto y fácilmente disponible las herramientas, códigos y protocolos para crear las Web y los contenidos propios. Los diversos debates en torno a su regulación intentaban ofrecer un marco normativo que asegurara que ningún actor discriminara, favoreciera, disminuyera o bloqueara los flujos de datos circulantes[44].

---

[42] Vanina Carboni, Ornela y Labate, Cecilia. América Latina por una red neutral: el principio de neutralidad in Chile y Brasil. 2018. Revista FAMECOS: mídia, cultura e tecnologia, vol. 25, núm. 2, consultado el 13 de enero de 2023. Disponible en: https://www.redalyc.org/jatsRepo/4955/495557631013/html/index.html#:~:text=El%20concepto%20de%20neutralidad%20de,garantizar%20la%20conexi%C3%B3n%20entre%20usuarios.

[43] Cit. Por Gendler, M. 2019. Neutralidad de la red y servicios *over the top*: una compleja relación en el ecosistema de telecomunicaciones. PAAKAT: revista de tecnología y sociedad, núm. 17, pp. 1-17. Consultado el 13 de enero de 2023. Disponible en: https://www.redalyc.org/journal/4990/499063348008/html/

[44] Gendler, M. 2019. Neutralidad de la red y servicios *over the top*: una compleja relación en el ecosistema de telecomunicaciones. PAAKAT: revista de tecnología y sociedad, núm. 17, pp. 1-17. Consultado el 13 de enero de 2023. Disponible en: https://www.redalyc.org/journal/4990/499063348008/html/

Con la aparición, veloz crecimiento y popularidad de diversas plataformas y empresas *Over The Top* (OTT)[45], el debate tomó nueva relevancia, ya que poco a poco estas fueron primando sobre otro tipo de interacciones en internet y crearon un gran volumen de datos circulantes que requería una fuerte inversión en las capas de infraestructura de internet para poder tolerarlas, inversión cubierta sobre todo por los proveedores de servicios de internet y, en algunas regiones, también por los Estados, pero no por estas OTT ni por los usuarios[46].

La neutralidad puede ser vista además como principio en el cual las personas podamos interactuar con la internet sin ningún tipo de discriminación con nuestra conexión entre plataformas, con otros usuarios, aplicaciones, *software, hardware* y los propios proveedores de servidores de internet; este principio garantiza una libre y diversa competencia en el mercado de la internet y también nos ofrece herramientas para que la sociedad en general pueda interactuar con libertad, sin restricciones y sin ningún tipo de discriminación en la era digital. Además, la mera existencia de libertad no significa necesariamente un especio digital libre de reglas. Todo lo contrario, de acuerdo con Quijano "se trata de establecer un marco que promueva el libre flujo de información para beneficio de la economía y la sociedad, que permita minimizar los daños y maximizar las ventajas de las TICs"[47].

La mera existencia de la NN no sólo beneficia a la población en general, sino también a las empresas y gobiernos, ya que entre empresas existe una mayor competitividad y libre acceso al mercado de la internet, evitando así la monopolización del mercado. En cuanto a los gobiernos, se garantiza que entre ellos no exista una vigilancia o espionaje para beneficios políticos, económicos y militares. Y entre gobiernos, empresas y sociedad en general se garantiza también

[45] Las empresas OTT más conocidas son aquellas que prestan servicios de comunicación equivalentes a los que ofrecen las operadoras. Los servicios de telefonía y mensajería se ven sustituidos con servicios como Skype o Whatsapp. Análogamente, algunos servicios como Netflix devoran el mercado de los contenidos multimedia por TV que ofrecen las operadoras de telecomunicación. Muñoz Igual, A. Las empresas Over-the-top y su impacto en el sector de las operadoras de telecomunicaciones Consultado el 14 de febrero de 2023. Disponible en: http://economiadigital.etsit.upm.es/wp-content/uploads/2015/12/AnaMunoz.pdf

[46] *Ibidem.*

[47] Quijano Decanini, Carmen. *Derecho a la privacidad en internet.* México. 2022. Colección Tirant 4.0., pág. 200.

que no haya una vigilancia a nuestras vidas privadas y/o exista información importante censurada.

1.10 Principios de la protección de datos personales

Como en casi todas las ramas del derecho y también en diversas disciplinas o áreas del conocimiento, los principios son necesarios porque establecen la razón de ser de tal o cual cosa. En el caso de los principios rectores de los datos personales, estos guían y dan pauta a un mejor entendimiento de la realidad actual, así como para entender cómo solucionar los problemas que llega a ocasionar el uso ilegitimo y desmedido de los datos personales.

Antes de conocer cuáles son los principios de datos personas, es necesario comprender qué es un principio. De acuerdo con Dworkin, un principio es "un estándar que ha de ser observado, no porque favorezca o asegure una situación económica, política o social que se considere deseable, sino porque es una exigencia de la justicia, la equidad o alguna otra dimensión de la moralidad"[48], dicho en otras palabras, los principios establecen que actuar de cierta manera es lo correcto y lo mejor para el ser humano. Esto debido en los principios se establecen los "lineamientos" que han de ser respetados para logar una buena convivencia entre las personas. Además, para Dworkin "los principios poseen una dimensión de peso o de importancia de la cual carecen las normas. Y es precisamente esta dimensión la que hace que los principios deban ser comparados entre sí, y el caso resuelto según el peso relativo atribuido a los diversos principios concurrentes"[49]
Para Portela, el concepto de principio jurídico "tiene que ver con algo "vago", "ideal", "absoluto", "pragmático" y que constituye básicamente una especie de puerta que comunica al derecho con la moral, a partir de invocaciones genéricas a la equidad y a la justicia"[50]. A modo de análisis, la suscrita concuerda con el anterior autor al

[48] Cit. Por Portela, Jorge Guillermo. Los principios jurídicos y el neoconstitucionalismo. Kíkaion, vol. 23, núm. 18, diciembre, 2009, pp. 33-54. Consultado el 12 de mayo de 2023. Disponible en: https://www.redalyc.org/articulo.oa?id=72012329003
[49] *Ibídem.*
[50] Portela, Jorge Guillermo. Los principios jurídicos y el neoconstitucionalismo. Kíkaion, vol. 23, núm. 18, diciembre, 2009, pp. 33-54. Consultado el 12 de mayo de 2023. Disponible en: https://www.redalyc.org/articulo.oa?id=72012329003

momento de referirse éste que los principios jurídicos son una puerta “ideal” y “pragmática” entre el derecho y la moral, porque los principios jurídicos son una excelente herramienta para el jurista que se aboca a defender un asunto en específico, y que cuando algunas normas jurídicas no le favorecen en su totalidad, los principios jurídicos tiene mucho que aportar para lograr posibles soluciones que le favorezcan a su caso en concreto; y para el juzgador o juzgadora, los principios jurídicos son una adecuada guía para determinado asunto.

Es importante resaltar que, para Dworkin, los principios por sí solos no constituyen verdaderas normas jurídicas. Estos necesariamente tienen que ser reconocidas por una norma de derecho positivo o por una sólida jurisprudencia[51].

En cuanto a la materia de la protección de datos personales, y además de los derechos ARCO, el marco legal establece varios principios rectores de la protección de los datos personales, mismos que se reconocen en casi todas las legislaciones. Estos principios no solo se traducen en obligaciones para quienes poseen los datos, sino también constituyen criterios de valoración frente a cualquier duda en el uso y manejo de estos[52].

La historia sobre los principios y normas legales para la protección de los datos personales en México no es mucha, sin embargo, atendiendo a las normas legales de otros países se puede notar que diversos países se dieron a la tarea de proteger a los internautas mediante algunas leyes nacionales específicas o convenios internacionales.

Se puede llegar a decir que de los primeros documentos a nivel internacional que comienza a describir los principios de los datos personales, fue el Convenio número 108 del Consejo de Europa para la Protección de las Personas con respecto del Tratamiento Automatizado de Datos de Carácter Personal, creado el 28 de enero

[51] C.f. en Suárez-Rodríguez, José Julián. El fundamento de los principios jurídicos: una cuestión problemática. Cvilicar. Ciencias Sociales y Humanas, vol. 16, núm. 30, enero-junio, 2016, pp. 51-61. Consultado el 12 de mayo de 2023. Disponible en: https://www.redalyc.org/articulo.oa?id=100246672002

[52] Quijano Decanini, Carmen. *Derecho a la privacidad en internet.* México. 2022. Colección Tirant 4.0., pág. 162.

de 1981, junto a un protocolo adicional relativo a las Transferencias de Datos, este firmado 2001.

a) Consentimiento.

Este principio es quizá de los más importantes para proteger los datos personales y en general para el ejercicio de cualquier otro derecho. En el ámbito del internet, deriva precisamente del derecho a la autodeterminación informativa y consiste en que el titular debe conocer y consentir la recolección, uso y transmisión de sus datos personales. La manifestación de la voluntad del titular debe de ser clara y precisa[53].

De acuerdo con la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), "*todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley. El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición*"[54]. A pesar de que la ley anteriormente citada tiene el principal objetivo de proteger los datos personales, vemos que la misma necesita una mejor y adecuación a las necesidades reales. En esta ley vemos que además de incluir excepciones a este principio, sólo se avoca en respetar un aviso de privacidad sin mencionar que los titulares de datos personales pueden tener la libre disposición de elegir qué cláusulas del aviso de privacidad se debe de aceptar. Cuando se hace uso de un servicio en la internet, muchas veces al ser necesario su uso, se acepta simplemente por el hecho de aceptar sin siquiera estar completamente de acuerdo con el aviso de privacidad, lo cual conlleva a un consentimiento parcial.

---

[53] *Íbidem*, pág. 168.

[54] Ley Federal de Protección de Datos Personales en Posesión de Particulares. Consultado el 09 de diciembre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
También está en González, A. (2011). "La protección de datos personales en la publicidad y el marketing en: México, España y Argentina". [Tesis de licenciatura, Universidad Nacional Autónoma de México]. Repositorio institucional de la Universidad Nacional Autónoma de México. http://132.248.9.195/ptb2011/mayo/0669181/0669181_A1.pdf

De acuerdo con la doctrina del derecho civil, en los meros convenios y contratos, se debe de atender al principio de consentimiento, con el cual, al existir este, los mismos se perfeccionan. Es decir, sin existir el consentimiento en los contratos o convenios (incluidos los digitales), se atiene a una causa de nulidad relativa. Esto muchas veces se produce porque en los contratos, convenios o, en este caso, los avisos de privacidad, hay falta de forma, existe error, dolo, mala fe, incluso por violencia, lesión o incapacidad[55].

Es complicado que en la realidad actual todos los contratos, convenios o avisos de privacidad sean totalmente claros en la forma en la que solicitan la manifestación de la voluntad.

b) Información.

El principio de información es básico y esencial en la materia de protección de datos personales, porque el responsable tendrá la obligación de informar a los titulares de los datos la información que se recabe de ellos y su finalidad[56]. El responsable deberá informar al titular, a través de aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto[57].

Este principio está estructurado prácticamente en casi todo el aviso de privacidad, porque es cuando se establecen los lineamientos en los cuales el titular acepta dar sus datos personales a un tercero, que se convierte en responsable.

c) Calidad de los datos.

Este principio también es conocido como “exactitud de los datos”. La exactitud y la precisión revisten una importancia vital para la protección de la privacidad. Los datos

[55] Código Civil del Estado de México, artículo 7.14. Consultado el 06 de diciembre de 2022. Disponible en: https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/cod/vig/codvig001.pdf

[56] Mendoza Enríquez, Olivia Andrea. Marco Jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. Revista IUS, vol. 12, núm. 41, 2018, Enero-Junio, pp. 267-291. Consultado el 14 de febrero de 2023. Disponible en: https://www.redalyc.org/journal/2932/293258387015/293258387015.pdf

[57] Artículo 26 LGPDPPSO.

inexactos pueden perjudicar tanto al encargado de datos como al titular, pero en una medida que varía mucho según el contexto[58].

El principio de calidad consiste en la obligación que tiene el responsable de adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que está tratando y se encuentren bajo su resguardo y posesión, a fin de que no se altere la veracidad de éstos y según se requiera para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que motivaron su tratamiento[59].

Se presume que se cumple con él principio de calidad en los datos personales, cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario[60].

d) Finalidad.

El principio de finalidad es una de las partes medulares para la protección de datos personales porque con la finalidad, todo tratamiento de datos que sea efectuado, el responsable tiene la obligación de justificar las finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera, o en el caso de empresas privadas, que el tratamiento de datos personales se limite al cumplimiento de las finalidades previstas en el aviso de privacidad[61].

---

[58] Principios Actualizados sobre la Privacidad y la Protección de los Datos Personales. Consultado el 09 de diciembre de 2022. Disponible en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

[59] Principios y deberes en materia de protección de datos personales. Consultado el 09 de diciembre de 2022. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/763381/Principios_y_deberes_en_materia_de_Proteccion_de_Datos_Personales.pdf

[60] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 09 de diciembre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

[61] Mendoza Enríquez, Olivia Andrea. Marco Jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. Revista IUS. ISSN: 1870-2147. Consultado el 14 de febrero de 2023. Disponible en: https://www.redalyc.org/journal/2932/293258387015/293258387015.pdf

De acuerdo con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), en su artículo número 18, "*el responsable podrá modificar las finalidades del tratamiento que se establecieron en un primer momento en el respectivo aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley para tales efectos y medie nuevamente el consentimiento del titular*"[62].

e) Proporcionalidad.

La proporción de los datos recabados es igual a la finalidad establecida en el aviso de privacidad. Así pues, resulta indispensable que los datos que son solicitados sean equivalentes sólo para ejecutar y cumplir las acciones que se necesitan para conseguir un fin determinado. Un primer acercamiento a una definición legal se proporciona en el artículo 13 de la LFPDPPP, el cual establece que "*el principio de proporcionalidad se refiere a que el tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de estos a efecto de que sea el mínimo indispensable*"[63].

Este principio se relaciona mucho con el principio de finalidad, ya que el encargado del requerimiento y tratamiento de los datos personales, deben de solicitar sólo los datos necesarios y pertinentes, esto de acuerdo con la finalidad que va a cumplir el tratamiento de los datos personales, logrando así una proporcionalidad en esta relación contractual. Lo anterior algunas veces es difícil de lograr, ya que, de acuerdo con el estudio de protección de datos personales entre usuarios y empresas, realizado por la Asociación Mexicana de Internet, solo 4 de cada 10 internautas revisan siempre o casi siempre el aviso de privacidad antes de

[62] Principios y deberes en materia de protección de datos personales. Consultado el 09 de diciembre de 2022. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/763381/Principios_y_deberes_en_materia_de_Proteccion_de_Datos_Personales.pdf

[63] Ley Federal de Protección de Datos Personales en Posesión de Particulares. Consultado el 12 de diciembre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

proporcionar sus datos[64], sin saber siquiera el uso que se les dará a sus datos recabados.

En conclusión, los datos recabados sólo deben de ser los necesarios. Y en caso de los datos sensibles, debe de requerirse el menor tiempo posible, además de que deben de mantenerse actualizados.

f) Responsabilidad.

Este principio resalta la importancia que tiene recabar, tratar y usar los datos de los titulares siempre de la mejor manera. Con este principio se puede exigir que los responsables del tratamiento de los datos tomen las medidas necesarias para que los datos de las personas no se sustraigan ilegalmente. Dichas medidas deberían ser auditadas y actualizadas periódicamente. El responsable o encargado del tratamiento y, en lo aplicable, sus representantes, deberían cooperar, a petición, con las autoridades de protección de datos personales en el ejercicio de sus tareas[65].

De acuerdo con el artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, el principio de responsabilidad establece que "*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*"[66]. Además, establece que "los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el

[64] Primer Estudio sobre Protección de Datos Personales entre Usuarios y empresas en México. Asociación Mexicana de Internet (AMIPCI). Consultado el 14 de diciembre de 2022.
También consultado por Arellano, C. (2020). El derecho de protección de datos personales. CJP, BIOLEX Y REVISTA CJP Número especial en conjunto, diciembre de 2020. Universidad Politécnica de Nicaragua y Universidad de Sonora. ISSN 2413-810X; ISSN 2007-5545; ISSN 2410-2768 | Págs. 127-136.
[65] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Organización de Estados Americanos. Consultado el 07 de diciembre de 2022. Disponible en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf
[66] Artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Consultado el 15 de febrero de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

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"[67].

En un estudio realizado por Asociación Mexicana de Internet, 187 empresas en México fueron evaluadas, de las cuales, el 100% de las evaluadas, dijo que guarda o almacena algún tipo de dato personal, de los cuales, 90% guarda datos principalmente de identificación. Y a pesar de que el 93% de las empresas dijo tomar en cuenta la política o herramientas de privacidad que ofrecen proveedores de Software y cómputo en la nube, sólo el 12% de las empresas encuestadas conoce con certidumbre la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su reglamento[68]. Por consiguiente, estos datos demuestran que, de las empresas encuestadas, son pocas las que conocen las consecuencias que les puede traer no implementar sistemas informáticos que garanticen la seguridad de los datos personales.

El principio de responsabilidad tiene un carácter transversal. Sin el cumplimiento de este, difícilmente se pueden cumplir los otros principios. Este principio, no sólo recomienda, sino que obliga a los responsables y encargados del tratamiento de datos personales a implementar, mejorar y mantener actualizados sus sistemas o infraestructura de datos para evitar alguna posible afectación a los titulares de los datos personales.

En el capítulo de conclusiones, se proporcionan una serie de recomendaciones tanto para organizaciones, empresas, instituciones públicas y a público en general para proteger sus datos personales y su derecho a la privacidad, sin embargo, es justo recordar la importancia y gran responsabilidad de los mismos responsables en conocer no sólo las leyes nacionales, sino también las internacionales para un mejor uso y tratamiento de los datos de los titulares. Esto sin lugar a duda, ahorraría mucho dinero y tiempo en el futuro para los responsables del tratamiento de datos.

---

[67] *Ibidem.*

[68] Primer Estudio sobre Protección de Datos Personales entre Usuarios y empresas en México. Asociación Mexicana de Internet (AMIPCI). Consultado el 15 de diciembre de 2022.

g) Licitud.

Este principio consiste en el pleno cumplimiento de la legalidad y respeto de la buena fe y los derechos del individuo. Se prohíbe recabar o conservar datos mediante engaño o fraude, de manera que el individuo no pueda conocer con propiedad los términos y condiciones del tratamiento. Para el titular de los datos debe quedar claro qué es lo que se está recabando, tratando o consultando. Toda información sobre el tratamiento de datos debe ser fácil de entender[69].

En la mayoría de los contextos se puede cumplir el requisito de legalidad si el recopilador o encargado de los datos personales informa al titular sobre las bases jurídicas de la solicitud de los datos en el momento de su recopilación (por ejemplo, "se solicita su número de identificación personal de conformidad con la Ley de Registro Nacional de 2004" o "la Directiva 33-25 del Ministerio de Economía"[70]. Además, la Organización de Estados Americanos (OEA), propone que para una mayor claridad en cuánto a la solicitud de los datos personales, se pretenda en lo máximo de lo posible, que se explique de manera precisa para que se solicita la información o los datos.

El principio de licitud, además se encuentra plasmado dentro de la LGPDPPSO, a través de su artículo 17, en el cual se establece el deber, por parte del responsable, de "llevar a cabo el tratamiento de datos personales conforme y en base a las facultades y atribuciones que la correspondiente normativa le confiera"[71].

[69] Quijano Decanini, Carmen. Derecho a la privacidad en internet. México. 2022. Colección Tirant 4.0., *op. Cit.* 167.
[70] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Organización de Estados Americanos. Consultado el 07 de diciembre de 2022. Disponible en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf
[71] Principios y deberes en materia de protección de datos personales. Consultado el 09 de diciembre de 2022. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/763381/Principios_y_deberes_en_materia_de_Proteccion_de_Datos_Personales.pdf

h) Lealtad.

La idea es respetar la expectativa razonable de privacidad, que es la confianza que deposita cualquier persona en otra respecto de que sus datos personales serán tratados conforme a lo acordado por las partes[72]. A través de este principio, además se busca que las empresas, organizaciones, gobierno y todo aquél que se dedique a la obtención y tratamiento de datos personales adopten una cultura de prevención a fraudes, engaños o extorsiones. Esto porque los titulares de los datos depositan su confianza con los responsables del tratamiento de sus datos.

El principio de lealtad no sólo es un principio, sino que es además una forma de actuar con ética y profesionalismo parte del responsable de la recopilación y tratamiento de los datos. El principio de lealtad es también en esencia, transversal al resto de los principios de protección de datos personales. El principio de lealtad requiere un actuar éticamente correcto no sólo en la recolección de los datos, sino también las herramientas, plataformas, mecanismos de defensa que los responsables de los datos den a los titulares de estos.

1.11 Otros principios sobre protección de datos personales

La legislación mexicana hace referencia a los principios de licitud, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad para el correcto cuidado de los datos personales, sin embargo, el objetivo de este trabajo de investigación es tener un alcance mayor en la comprensión de los derechos digitales, es por esto por lo que, no sólo se atiende a principios de leyes nacionales, sino que además se proporcionan principios recomendados por organizaciones internacionales.

a) Seguridad de los datos

En un primer término, antes la seguridad se enfocaba a la protección de la vida sólo en “la vida real”, ahora este derecho y evoluciona al igual que otros derechos o

[72] Quijano Decanini, Carmen. Derecho a la privacidad en internet. México. 2022. Colección Tirant 4.0., pág. 173.

conceptos para convertirse en un derecho digital. La seguridad como derecho humano se hace necesaria en cualquier aspecto de nuestras vidas. La seguridad humana implica libertad frente a las privaciones, libertad frente al miedo y libertad para actuar en nombre propio[73].

De acuerdo con los Principios sobre Privacidad y la Protección de Datos Personales establecidos por el Comité Jurídico Interamericano de la OEA, los responsables de los datos "deberían establecer y mantener las medidas de carácter administrativo y técnico que sean necesarias para establecer salvaguardias de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los Datos Personales que obren en su poder o bajo su custodia (o de los cuales son responsables) y cerciorarse de que tales Datos Personales no sean tratados ni divulgados excepto con el consentimiento de la persona o de otra autoridad legítima, ni sean accidentalmente perdidos, destruidos o dañados[74]. Los medios técnicos (incluyendo programas, plataformas, servicios, etc.) son los principales en necesitar una arquitectura de seguridad sólida, fuerte y eficaz. Asimismo, el personal de aquellos responsables o encargados del tratamiento de los datos personales, requieren una actualización constante sobre las buenas prácticas y la normatividad nacional e internacional sobre el adecuado tratamiento de datos.

El uso e incremento de los medios y herramientas digitales crecieron significativamente desde la pandemia global del SARS-CoV-2 del 2020 en todo el mundo, tan solo en México y en el 2021, se cuenta con 88.6 millones de internautas, lo cual representa el 75.6% de la población de 6 años o más[75], por lo que se

[73] Leal Moya, Leticia. (2005). Seguridad humana: La responsabilidad de proteger. *Boletín mexicano de derecho comparado*, *38*(114), 1117-1138. Recuperado en 15 de diciembre de 2022, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332005000300005&lng=es&tlng=es.

[74] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Organización de Estados Americanos. Consultado el 07 de diciembre de 2022. Disponible en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

[75] 18º Estudio sobre los hábitos de Personas Usuarias de Internet en México 2022. Consultado el 15 de diciembre de 2022. Disponible en: https://irp.cdn-website.com/81280eda/files/uploaded/18%C2%B0%20Estudio%20sobre%20los%20Habitos%20de%20Personas%20Usuarias%20de%20Internet%20en%20Mexico%202022%20%28Socios%29%20v2.pdf

convierte importante que la sociedad en general adquiera conocimientos básicos sobre sus derechos digitales; también sobre los mecanismos legales que les permitan acceder, rectificar, cancelar u oponerse al tratamiento de sus propios datos personales.

En términos generales, las medidas adoptadas para proteger los Datos Personales deberían ser elegidas tomando en cuenta, entre otros factores: i) la posible afectación a los derechos de los Titulares, en particular, el posible valor de los datos para una tercera persona no autorizada para su tratamiento; ii) los costos de su implementación; iii) las finalidades del tratamiento, y iv) la naturaleza de los Datos Personales tratados, en especial los Datos Sensibles. La índole de las salvaguardias implementadas podría variar según la sensibilidad de los datos en cuestión. Evidentemente, los Datos Sensibles requieren un nivel más alto de protección, a la luz de riesgos como, por ejemplo, la usurpación de la identidad, pérdidas económicas, efectos negativos en la calificación crediticia, daños a bienes y pérdida del empleo o de oportunidades comerciales o profesionales, la vulneración de la intimidad sexual, o actos de violencia de género digital[76].

Al mismo tiempo, es importante considerar que en la legislación mexicana se considere el deber de las organizaciones, empresas, gobierno o cualquiera que se dedique al tratamiento de datos, a notificar a las autoridades dedicadas a solucionar los problemas legales derivados de los tratamientos no autorizados o ilegítimos, así como la pérdida, destrucción, daños o divulgación de los datos personales (incluso cuando haya sido de manera accidental). Esto permitiría que los titulares actuarán rápidamente para proteger su integridad y evitar un detrimento a sus derechos humanos.

[76] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Consultado el 15 de diciembre de 2022. Disponible en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

b) Transferencia Internacional de datos

En un mundo globalizado, para las organizaciones, gobierno y, sobre todo las empresas, la transferencia internacional de datos se vuelve cada vez más necesaria. Sin embargo, las leyes referentes a la transferencia internacional siguen siendo confusas, porque las leyes de los distintos países que mantienen comunicación política, cultural, económica y social es diferente entre sí, lo cual da a la posibilidad de confusión entre los mismos y, cuando existe alguna controversia, hasta cierto punto resulta difícil encontrar la mejor manera de resolver un problema referente a la transmisión de los datos.

Desde el punto de vista técnico-jurídico, habrá que entender como transferencia internacional de datos aquella que se da cuando exista comunicación por transmisión, difusión o cualquier otra forma de puesta a disposición de datos[77] entre un país que obtiene de manera directa los datos personales (responsable) y otro país distinto de la jurisdicción del responsable.

Este principio, se estable en México en su Ley Federal de Protección de Datos Personales en Posesión de Particulares, partir del artículo 36 y hasta el artículo 37, sin embargo, su redacción es confusa. Primero que nada, la legislación menciona en forma muy breve sobre la transferencia “internacional”, y un poco más sobre la transferencia nacional. También establece excepciones las cuales resultan un poco contradictorias a los mismos principios de que se establece en su misma ley. Por ejemplo, el artículo 37 de la misma Ley establece una excepción interesante, la cual está redactada de la siguiente manera: “artículo 37.- Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos: VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular”[78], pero esta redacción mantiene una laguna legal, porque

[77] Blas, F. (2009). Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales. Revista Derecho del Estado, (23),37-66. [fecha de Consulta 19 de Diciembre de 2022]. ISSN: 0122-9893. Recuperado de: https://www.redalyc.org/articulo.oa?id=337630233002

[78] Ley Federal de Protección de datos personales en Posesión de Particulares. Consultado el: 15 de diciembre de 2022. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

no se especifica bajo qué circunstancias se realizará esa transferencia (nacional o internacional).

Este trabajo no pretende proponer la eliminación del tratamiento y transferencia de los datos personales, en su lugar, pretende dar a conocer qué existen vacíos y lagunas legales que pueden provocar un mal tratamiento de los datos personales. Al contrario, la transferencia internacional de datos ayuda enormemente a mejorar la economía de un país, al permitir que las empresas mejoren sus servicios y productos; también se contribuye en la persecución de los delitos y conflictos jurídicos transfronterizos; siempre y cuando empresas, gobierno, o cualquier responsable del tratamiento de los datos, respeten el derecho a la privacidad y los derechos humanos.

En una realidad actual en la que tan sólo en México, existen 88.6 millones de internautas que representan el 75.6% de la población de 6 años o más[79] es necesario que se garantice un correcto tratamiento de los datos de los titulares, para evitar que los derechos humanos de los mismos sean vulnerados. Implica un reto que México y la mayoría de los países del mundo logren una armonía de leyes para una mejor protección de los datos personales. Además de establecer bases que logren conciliar y solucionar de manera efectiva posibles problemas por la transferencia nacional o internacional de datos.

c) Deber de confidencialidad

La confidencialidad es un principio básico, sobre todo en una relación contractual. Este principio no se encuentra descrito explícitamente en la ley mexicana, sólo de manera somera. Aun así, es importante que los responsables y encargados del tratamiento de los datos personales sean conscientes de lo que implica este principio, para que así ejecuten de mejor manera sus actividades relacionadas con los datos personales.

[79] 18° Estudio sobre los Hábitos de Personas Usuarias de Internet en México 2022. Asociación de Internet. Mayo 2022. Consultado el 19 de diciembre de 2022.

Este deber requeriría que el responsable de Datos se cerciore de que no se proporcionen tales Datos (ni se pongan a disposición por otros medios) a personas o entidades excepto con el consentimiento de la persona, en consonancia con las expectativas razonables de la persona afectada o por mandato de la ley. En este último caso, la ley podría autorizar dicha divulgación para para garantizar el cumplimiento de obligaciones contractuales y legales, la protección de intereses públicos y privados legítimos[80]. En este caso, la excepción al deber de confidencialidad en los casos en los que la ley lo permite se debe mencionar de manera explícita y concreta en qué casos la información del titular de los datos personales dejan de ser confidenciales.

Además, este principio implica que el responsable garantiza un adecuado y eficiente sistema de seguridad en la que, en cualquier fase del tratamiento o administración de los datos personales, la información no será tratada sin el consentimiento del titular, evitando así posibles *hackeos*[81] a los sistemas de información de los encargados de los datos personales.

Este principio tiene mucha importancia cuando se velan por los intereses públicos y privados de un Estado o grupo de personas. Una pregunta interesante es: ¿sobre los intereses de quién o quiénes es que se omite la confidencialidad de la información de una o varias personas?, ¿al omitir la confidencialidad de la información, se vela por un interés público, o es en realidad un interés privado? Garantizar la confidencialidad no sólo es una cuestión de legalidad, sino también de ética.

[80] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Pág. 45 Organización de Estados Americanos. Consultado el 15 de diciembre de 2022. Disponible en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

[81] El hackeo consiste en poner en riesgo sistemas informáticos, cuentas personales, redes de ordenadores o dispositivos digitales. Consultado el 15 de febrero de 2023. Disponible en: https://www.avg.com/es/signal/what-is-hacking#:~:text=El%20hackeo%20consiste%20en%20poner,la%20definici%C3%B3n%20oficial%20de%20hackeo.

d) Tratamiento y conservación limitados.

Este principio se relaciona en parte y principalmente con el principio de finalidad. Los datos personales deben de ser tratados sólo con la finalidad estipulada dentro del aviso de privacidad o convenio. Además, su conservación no debería exceder del tiempo necesario para cumplir dichas finalidades, de conformidad con la legislación nacional correspondiente[82]. Si se requiere dar otro uso respecto con el fin estipulado, los responsables deben avisar a los titulares de los datos para que ellos estén enterados para qué y cómo será usada su información. En este nuevo aviso hacia los titulares de los datos, deben de obtener un consentimiento expreso o tácito, de acuerdo con las especificidades de la ley.

Existen algunas excepciones específicas las cuales no requieren de un consentimiento expreso o tácito de los titulares de los datos para su tratamiento, esto puede ser para salvaguardar la seguridad nacional y/o internacional, por motivos de salud, para cumplir con obligaciones legales, entre otras. Aun así, y a manera de obligación, los responsables deben respetar en todo momento el respeto a los derechos humanos de los titulares de los datos.

Para la conservación de los datos, esto debe de hacerse por el menor tiempo posible y sin que afecte de ninguna manera los derechos de los titulares. Una vez alcanzado el fin para el cual los datos fueron recopilados, estos deben dejar de conservarse, a excepción de algunas consideraciones específicas como las mencionadas en el párrafo anterior. Sin embargo, no siempre es así. Hoy en día, los responsables y encargados del tratamiento de datos aprovechan que el costo del almacenamiento de datos ha disminuido considerablemente, ya que suele ser menos costoso para los responsables de datos almacenarlos indefinidamente en vez de examinarlos y borrar los que no sean necesarios[83]. En consecuencia, se

[82] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Pág. 45 Organización de Estados Americanos. Consultado el 15 de diciembre de 2022. Disponible en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf.
[83] Ibidem, pág. 43.

hace una conservación innecesaria y/o excesiva de datos que impide el respeto a la vida privada.

1.12 Derechos ARCO.

Uno de los principales mecanismos legales en México, para el ejercicio de los derechos digitales son los derechos ARCO. Estos derechos son ejercidos directamente por los titulares de los datos personales o por su representante legal. La forma de ejercer estos mecanismos legales se explica en el capítulo IV del presente trabajo de investigación.

Los derechos ARCO surgen en 2009 de la reforma constitucional al artículo 16, donde reconoce que todas las personas tienen derecho al acceso, rectificación, cancelación u oposición de sus datos personales. La ley reglamentaria de este párrafo constitucional es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares[84], además de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y su respectivo Reglamento.

a) Derecho de acceso.

La doctrina define al derecho de acceso como el que corresponde a todo individuo para solicitar y obtener gratuitamente información sobre sus datos, el origen de estos, así como las transmisiones o comunicaciones realizadas o que se pretendan hacer de dichos datos[85].

Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), en su artículo 44, define el derecho de acceso de la siguiente manera: “El titular tendrá derecho de acceder a sus datos personales

[84] Recht Legal. ¿Cómo ejercer el derecho al “olvido” en México? Consultado el 11 de enero de 2023. Disponible en: https://recht.com.mx/ejercer/#:~:text=Los%20derechos%20ARCO%20surgen%20en,oposici%C3%B3n%20de%20sus%20datos%20personales.

[85] Quijano Decanini, Carmen. Derecho a la privacidad en Internet. 2022. Tirant lo blanch, México. Pág. 162.

que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento”[86].

b) Derecho de rectificación.

Este derecho es la facultad del titular de los datos personales de exigir que el responsable del tratamiento mantenga sus datos en correcto estado, es decir, que se encuentren actualizados, no estén incompletos o sean inexactos. Este derecho de rectificación es además un recordatorio para que los responsables mantengan sus bases de datos actualizados.

Por su parte, la LGPDPPSO, en su artículo 45, define el derecho de rectificación como “*aquel en el cual el titular tiene derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cundo estos resulten ser inexactos, incompletos o no se encuentren actualizados*”[87]

c) Derecho de cancelación.

De acuerdo con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), el derecho de cancelación es aquel en el cual el titular cancela sus datos personales. El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último[88].

Si los datos hubiesen sido transmitidos a un tercero antes de la fecha de rectificación o cancelación, el responsable debe dar aviso al tercero de dicha solicitud de cancelación o rectificación por parte del titular de los datos personales, y proceda a cancelar o rectificar.

---

[86] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 11 de enero de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

[87] *Idem.*

[88] Artículo 46 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 11 de enero de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

El derecho de cancelación es el derecho de todo individuo para que se supriman los datos que sean inadecuados o excesivos, lo cual permitirá el bloqueo de los mismos o para que se cancelen o eliminen cuando ya no son necesarios para el cumplimiento de la relación jurídica para la cual fueron proporcionados[89].

d) Derecho de oposición.

La LFPDPPP en su artículo 27 define a este derecho como aquel en el cual *"el titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular"*[90].

Este derecho es la facultad que tiene el titular de solicitar que cualquier persona física o moral se abstenga de utilizar su información personal para ciertos fines, siempre que medie causa legítima o que el uso de la información personal del titular signifique un menoscabo a su persona y sus derechos.

Una vez analizados los conceptos elementales para comprender la materia de la protección de datos personales, los siguientes capítulos se avocarán a describir de manera más detalla ejemplos reales que involucran el uso cotidiano de los datos personales en las nuevas tecnologías y en la internet. Asimismo, se analizarán los mecanismos legales nacionales e internacionales existentes para ejercer nuestro derecho a la protección de datos personales y la vida privada.

[89] Quijano Decanini, Carmen. Derecho a la privacidad en Internet. 2022. Tirant lo blanch, México. Pág. 162.
[90] Artículo 27 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares Consultado el 15 de febrero de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

CAPÍTULO II. EL FLUJO DE LOS DATOS EN LA ERA DIGITAL

2.1 Uso para fines económicos

La tecnología crea y supera nuevas formas de relacionarnos. Desde la educación, la medicina, el entretenimiento, el trabajo, y claro, la manera de hacer negocios. Por ejemplo, los corredores de data, o *data brokers,* se refieren a empresas dedicadas a recolectar datos personales de múltiples fuentes para ofrecer productos que se derivan de la venta directa de datos o de su análisis. Este tipo de negocio no es nuevo; las empresas de marketing recolectan información demográfica y sobre los intereses de grupos poblacionales para ofrecer publicidad dirigida por medios impresos o telefónicos[91].

Bajo este escenario las formas de recolectar los datos personales son muchas y muy variadas. Los corredores de data, a través de las tecnologías de rastreo (TR), obtienen los datos por medio de las *cookies*[92]; y estas, a su vez, son obtenidas por casi todas las plataformas que usamos. Desde aquellas plataformas para realizar compras en línea, hasta las aplicaciones que utilizamos para jugar. Además, las cookies son obtenidas por distintos sectores, como el público, el privado y las asociaciones. En consecuencia, González afirma que:

> *"En este contexto, también se agregan datos de las actividades comerciales de las personas. Las tiendas venden e intercambian información sobre prácticas de consumo, como las ventas por catálogo, las suscripciones o revistas, ventas de automóviles, encuestas de marketing, tarjetas de clientes frecuentes, entre otras. Por ejemplo, los corredores de datos de Oracle y Datalogix afirman agregar y proveer*

[91] González, L. (2018) Control de nuestros datos personales en la era del *big data:* el caso del rastreo web de terceros. Revista Estudios Socio-jurídicos, vol. 21, núm. 1, pp.209-244. Consultado el 23 de enero de 2023. Disponible en: https://www.redalyc.org/journal/733/73357886009/html/

[92] Una cookie (galleta o galleta de información) es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador. Consultado el 23 de enero de 2023. Disponible en: https://www.clacso.org/que-son-las-cookies/#:~:text=Una%20cookie%20(galleta%20o%20galleta,la%20actividad%20previa%20del%20navegador.

información sobre más de 2 billones de dólares en consumo de 110 millones de hogares, proporcionada por 1500 socios de datos"[93].

Es importante destacar que, con estas *cookies*, se pueden obtener perfiles de conducta, y estos a su vez son comercializados entre distintas empresas, de distintos tamaños y sectores, incluso entre el gobierno. Para las empresas, la comercialización de datos es una de las principales fuentes de ingresos, ya que las plataformas que se usan día con día, y de manera "gratuita", generan millones de datos en tan poco tiempo. Esta compleja actividad, genera enormes ganancias a las empresas tecnológicas.

Otro factor que posibilita la comercialización de millones de datos a nivel mundial se debe al gran avance que existe sobre el *big data*. Podría decirse que *big data* se refiere a "datos a gran escala" o "datos masivos". A pesar de que no existe una definición unívoca, el Observatorio de Bioética y Derecho de la Universidad de Barcelona lo define así: "Big Data es un término que designa el tratamiento de grandes volúmenes de datos mediante algoritmos matemáticos con el fin de establecer correlaciones entre ellos, predecir tendencias y tomar decisiones"[94]. Este tratamiento de los "datos masivos" vino para crear una manera distinta de concebir las relaciones humanas. Los anterior, es eficiente, más económico, y mejor para nuestro día a día, empero, cuando estos millones de datos son usados y tratados de manera injusta, sin consentimiento del titular, y desproporcional a los principios sobre la protección de los datos personales, puede simbolizar una amenaza para el titular de los datos.

Cada día se generan 2,5 quintillones de bytes de datos, y si bien no es fácil imaginar lo que supone esa gran cantidad de datos[95]. Mayer-Schönberger y Cukier dan ejemplos abstractos sobre la cantidad de datos que se generan, argumentan que "si estuvieran

[93] González, L. (2018) Control de nuestros datos personales en la era del *big data:* el caso del rastreo web de terceros. Revista Estudios Socio-jurídicos, vol. 21, núm. 1, pp.209-244. Consultado el 23 de enero de 2023. Disponible en: https://www.redalyc.org/journal/733/73357886009/html/

[94] Observatorio de Bioética y Derecho, Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública, Universidad de Barcelona, 2015. Consultado el 24 de enero de 2023. Disponible en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf

[95] Soto, Y. Datos masivos con privacidad y no contra privacidad. 2017. Universidad Autónoma de Barcelona. Consultado el 24 de enero de 2023. Disponible en: https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872017000200008

impresos en libros, cubrirían la superficie entera de Estados Unidos, formando cincuenta y dos capas y si esta inmensa cantidad de datos estuvieran grabados en CD-ROMs apilados, tocarían la Luna formando cinco pilas separadas[96].

Hoy en día, las empresas innovan sobre la manera de comercializar esos datos. Por ejemplo, esto se puede notar en la publicidad, que es una de las principales maneras de hacer negocios entre las empresas de *streaming*, empresas de servicios, plataformas comerciales, aplicaciones, juegos en línea, redes sociales, entre otros. Los dividendos recibidos por la publicidad permiten no generar cobros al consumidor por el uso de contenidos y servicios en línea. Como se pueden cobrar precios más altos por la publicidad personalizada que por la publicidad generalizada, se incentiva recolectar mayor información de las personas para hacer perfiles comerciales lo más detallados posibles[97]. De acuerdo con Angwin, "para 2010, el costo promedio de un anuncio personalizado o dirigido era de US$4,12 por cada mil espectadores, en comparación con U$1,98 por cada mil espectadores de un anuncio no personalizado"[98].

Siendo así que las distintas maneras de recolectar e intercambiar la información sobre los datos personales son muchas para luego usarla en publicidad u otros fines, Arvind "señaló cinco formas en las que la identidad de un usuario es captada por las compañías, ya sean aquellas que tiene un primer acercamiento con el usuario o aquellas terceras compañías que compran esos datos a los primeros. Esas formas son las siguientes:

- Una tercera parte también es una primera parte, por ejemplo, Facebook, Twitter o Google+
- Una primera parte entrega (´filtra´) información de identificación a un tercero.

[96] Cit. por Soto, Y. Datos masivos con privacidad y no contra privacidad. 2017. Universidad Autónoma de Barcelona. Consultado el 24 de enero de 2023. Disponible en: https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872017000200008

[97] González, L. (2018) Control de nuestros datos personales en la era del *big data:* el caso del rastreo web de terceros. Revista Estudios Socio-jurídicos, vol. 21, núm. 1, pp.209-244. Consultado el 23 de enero de 2023. Disponible en: https://www.redalyc.org/journal/733/73357886009/html/.

[98] Cit. Por González, L. (2018) Control de nuestros datos personales en la era del *big data:* el caso del rastreo web de terceros. Revista Estudios Socio-jurídicos, vol. 21, núm. 1, pp.209-244. Consultado el 23 de enero de 2023. Disponible en: https://www.redalyc.org/journal/733/73357886009/html/

- Un tercero compra información de identificación de un ´servicio de correspondencia´.
- Un tercero explota una vulnerabilidad de seguridad para conocer la identificación de un usuario.
- Un tercero ´desanonimiza´ sus datos comparándolos con datos identificados."[99]

Nuestros pasos en internet se generan con cada "*click*" que hagamos en la internet. Por eso es importante prestar a atención a la manera en que se navega en la red.

a) El uso de los datos personales en la mercadotecnia

Para entender cómo los datos personales son usados por la mercadotecnia, es importante entender qué es mercadotecnia o "marketing". Una definición acorde con la era digital conlleva a citar a la American Marketing Association (AMA), "marketing es la actividad, el conjunto de instituciones y procesos para crear, comunicar, entregar e intercambiar ofertas que tienen valor para consumidores, clientes, socios y la sociedad en general[100]. Esta idea se usa para describir la actividad de la mercadotecnia en un ambiente tradicional como en uno digital.

Hoy en día, y principalmente las grandes empresas, utilizan el marketing y neuromarketing para satisfacer o crear necesidades humanas. Estas necesidades, originales o creadas, son obtenidas al analizar el comportamiento humano a través de diversas fuentes, como las redes sociales, las cámaras de vigilancia en los centros comerciales, en las llamadas telefónicas y en general, por la forma en que navegamos en la internet. En una sociedad de consumo las grandes compañías internacionales usan millones de datos analizados con métodos científicos para manipular nuestras emociones sin que nos demos cuenta. De ahí que Morales argumente:

[99] Traducido por la autora. Cit. por Mayer, J. Tracking the trackers: where everybody knows your username. 2011. CIS The Center for Internet and Society. Consultado el 26 de enero de 2023. Disponible en: https://cyberlaw.stanford.edu/blog/2011/10/tracking-trackers-where-everybody-knows-your-username#pii_leakage_footnote_1

[100] Ortiz Morales, M. D., Joyanes Aguilar, L., & Giraldo Marín, L. M. (2015). Los desafíos del marketing en la era del big data. *E-Ciencias De La Información*, *6*(1), 1–31. Consultado el 25 de enero de 2023. Disponible en: https://doi.org/10.15517/eci.v6i1.19005

> *"En esta era digital y de un cambiante entorno económico, es deber de las empresas indagar en los gustos de los clientes, realizar investigaciones de mercados y saber las actuaciones de la competencia con el objetivo principal de lanzar productos y servicios que les generen mayores ingresos. En otras palabras, la información cada día es más relevante para las compañías para la toma de decisiones. Las compañías no sólo necesitan recopilar datos, sino también buscar la forma adecuada de analizarlos para concebir actuaciones diarias fundamentales en estadísticas y tendencias"*[101].

Un estudio realizado por la CIS The Center for Internet and Society en 2011, muestra como las empresas, además de intercambiar y comercializar la información de sus usuarios, pueden llegar a experimentar un tipo de "fuga" de información, la cual, en lenguaje coloquial implicaría lo no intencional. Sin embargo, en seguridad informática, la fuga es un término técnico para un flujo de información: algunos casos de fuga son totalmente intencionales[102]. En este estudio, se muestra que la principal fuga de información es el nombre de usuario o el ID. Por ejemplo, ver un anuncio local en el sitio web de Home Depot envió el nombre y la dirección de correo electrónico del usuario a 13 empresas. Ingresar la contraseña incorrecta en el sitio web del Wall Street Journal envió la dirección de correo electrónico del usuario a 7 empresas. Interactuando con classmates.com envió el nombre y apellido del usuario a 22 empresas[103].

La razón por la cual las personas ceden, a veces sin saberlo, muchos de sus datos personales son porque conviven en el día a día con la internet, la inteligencia artificial (IA)[104], los teléfonos, relojes, pantallas y casas inteligentes. Por poner unos ejemplos, "Google, cuyo número de usuarios sobrepasa los mil millones, dispone de un

---

[101] *Ibidem.*

[102] Mayer, J. Tracking the trackers: where everybody knows your username. 2011. CIS The Center for Internet and Society. Traducido por la autora. Consultado el 26 de enero de 2023. Disponible en: https://cyberlaw.stanford.edu/blog/2011/10/tracking-trackers-where-everybody-knows-your-username#pii_leakage_footnote_1

[103] *Ibidem*. Traducido por la autora.

[104] De acuerdo con Oracle, la inteligencia artificial se refiere a sistemas o máquinas que imitan la inteligencia humana para realizar tareas y pueden mejorar iterativamente a partir de la información que reocpilan. Oracle. ¿Qué es la inteligencia artificial? Obtén más información sobre la inteligencia artificial. Consultado el 9 de marzo de 2023. Disponible en: https://www.oracle.com/mx/artificial-intelligence/what-is-ai/

impresionante número de sensores para espiar el comportamiento de cada usuario: el motor *Google Search* le permite saber dónde se encuentra el internauta, qué busca y en qué momento. El navegador *Google Chrome* envía directamente a *Alphabet,* la empresa matriz de *Google*, todo lo que hace el usuario en materia de navegación. *Google Analytics* elabora estadísticas muy precisas de las consultas de los internautas en la Red. *Google Maps* identifica el lugar en el que se encuentra el internauta, adónde va, cuándo y con qué itinerario. Y desde el momento en que la gente enciende un *Smartphone* con *Android*, *Google* sabe inmediatamente dónde está el usuario y qué está haciendo. Claro, nadie obliga a recurrir a *Google*, pero cuando se requiere, *Google* lo sabe todo sobre los usuarios"[105].

En consecuencia, al ver productos por internet, y sobre todo páginas de compras online, las empresas de internet recurren a diversas técnicas para generar mayor consumo ente la población. Es por eso por lo que, en los últimos años, mucha gente en el mundo adquirió hábitos innecesarios de consumo. Y es que a pesar de que en muchas ocasiones esos hábitos de consumo impulsivos y excesivos de las personas son "voluntarias", en realidad son aquellas compañías tecnológicas las que se dedican a recopilar, analizar, tratar y comercializar los datos de los titulares. Por consiguiente, terminan implantando la idea de un hiperconsumo en la sociedad. Esto, se logra a través de distintos medios digitales y no digitales que se expusieron anteriormente. Esta necesidad de comprar, hacer o dejar de hacer, es creada, en la mayoría de los casos, por las empresas en general que mejor saben explotar y comercializar nuestros datos.

Un ejemplo que ilustra mejor la idea anterior es dado por Mayer-Schönberger y Cukier, donde explican que "MasterCard tiene una división llamada MasterCard Advisors que agrega y analiza 65.000 millones de transacciones de 1.500 millones de titulares de tarjetas en doscientos diez países con la finalidad de definir tendencias de negocio y consumo. Luego vende esa información a otros. Entre otras cosas, descubrió que cuando la gente llena de gasolina el depósito del coche alrededor de las cuatro de la tarde existe la probabilidad de que, a lo largo de la hora siguiente, gasten de treinta y cinco a

[105] SOTO, Y., (2017). Datos masivos con privacidad y no contra privacidad. Revista de Bioética y Derecho, (40),101-114. Consultado el 27 de enero de 2023. ISSN 1886-5887. Disponible en: https://www.redalyc.org/articulo.oa?id=78351101008

cincuenta dólares en una tienda de comestibles o en un restaurante"[106]. Un publicista podría hacer uso de esa información para imprimir cupones de oferta de los negocios vecinos al dorso de los recibos de la gasolinera alrededor de esa hora del día. Como empresa intermediaria de los flujos de información, MasterCard se halla en una posición privilegiada para recopilar datos y capturar su valor. Se puede imaginar un futuro en el que las entidades emisoras de tarjetas de crédito renuncien a sus comisiones sobre las transacciones y las procesen gratuitamente a cambio de acceder a más datos, y perciban ingresos de la venta de analíticas cada vez más sofisticadas basadas en estos mismos datos"[107]. Mayer-Schönberger y Cukier no estaban equivocados cuando dijeron que estas empresas, como MasterCard, se encuentran en una posición privilegiada, ya que en efecto lo están. Esta venta de datos a gran escala no siempre tiene su lado bueno. Queda claro que no sólo se afecta a la privacidad de las personas a transferir sus datos personas a terceras partes; sino que, además, se llega a generar un consumismo desmedido y la consolidación de grandes monopolios empresarias y de datos. Estas mismas empresas que recogen, tratan y analizan los datos, no sólo son usados por ellos mismos y por terceros con fines económicos; como se leerá más adelante, otras empresas compran esos datos para después vender al gobierno cierta información de las personas: analizar su comportamiento, establecer patrones de comportamiento, identificar ideologías políticas, temas de polarización, entre otros. En el peor de los casos, está mega información de las personas resulta una manera de lograr controlar o reprimir a las personas e influir en sus decisiones.

La sociedad en general debe de estar consciente del gran valor que tiene su información personal. Por ello, es importante que la misma sociedad se interese por estos temas. Este trabajo no propone eliminar el acceso total a los datos personales, al contrario, del análisis de los datos surgen impresionantes progresos e inventos en el ámbito de la medicina, la educación, la energía, la alimentación, el entretenimiento, entre muchas otras áreas de estudio; en cambio, este trabajo de investigación pretende mostrar que en la actualidad existe deficiencia en la cultura de la privacidad y protección de los datos

[106] Cit. por SOTO, Y., (2017). Datos masivos con privacidad y no contra privacidad. Revista de Bioética y Derecho, (40),101-114. Consultado el 27 de enero de 2023. ISSN 1886-5887. Disponible en: https://www.redalyc.org/articulo.oa?id=78351101008
[107] *Ibidem*.

personales en la era digital. Además, pretende incentivar el reforzamiento y actualización de las bases jurídicas mexicanas, para logar que sean suficientes, fuertes y eficaces para ayudar al titular de los datos cuando éste se encuentre o haya sido vulnerado en sus derechos humanos y derechos digitales. Pretende, además, que la sociedad en general sea consciente sobre sus elecciones en su vida diaria. Y que no sea fácilmente manipulable por compañías, el gobierno, u otras personas.

b) ¿Ventajas o desventajas del uso de nuestros datos personales por parte de las empresas?

Ha diferencia de otros países, México no mantiene actualizadas sus leyes en las cuales se garantice un adecuado tratamiento de los datos personales. Lo anterior, deja en un estado de indefensión a la población en general, ya que no se marcan límites jurídicos a las empresas nacionales y extranjeras que recopilan, tratan y transfieren los datos personales de los titulares. También, no se establecen estándares mínimos para el buen actuar de las instituciones y personal dependiente del servicio público.

El establecer parámetros legales beneficia a la sociedad en general. Por ello se debe voltear a ver a países que tienen un mayor estudio y avance en la creación de normas jurídicas que regulen y prevengan futuros daños causados por la internet o el avance de la tecnología hacia las personas. Un ejemplo de ello es la Carta de Derechos Digitales de España[108], la cual hace una serie de recomendaciones no para prohibir el uso de los datos personales, sino para hacer eficiente y mejorar su tratamiento, sin que implique un daño a los derechos humanos de los titulares. Por su parte, La Unión Europea tiene actualizada la normativa sobre la protección de datos personales. Un ejemplo de ello es el reglamento General de la Unión Europea de Protección de Datos Personales (RGDP), el cual, comenzó a entrar en vigor el 25 de mayo de 2018[109]. Uno de los objetivos de este

[108] Carta de Derechos Digitales. Plan de Recuperación, Transformación y Resiliencia. Gobierno de España. Consultado el 18 de enero de 2023. Disponible en: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

[109] Reglamento (EU) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. Consultado el 18 d enero de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

nuevo reglamento es impulsar en la Unión Europea el creciente mercado digital, así como potenciar su uso social, sin que implique sacrificar alguno de los principios sobre la protección de los datos personales.

El derecho no avanza a la par que la tecnología, por eso, estos avances requieren un marco más sólido y coherente para la protección de datos, respaldado por una ejecución estricta y de cooperación internacional, dada la importancia de generar confianza que permita a la economía digital desarrollarse en todo el mercado. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades[110].

Una manera en que las empresas logren ser competitivas entre sí es generar confianza entre sus clientes o usuarios. Las mismas empresas deben reforzar su compromiso para con los clientes sobre la protección de sus datos personales. Una manera de lograrlo es a través del mantenimiento y mejora constante sobre los programas técnicos y capacitación al personal encargado del tratamiento de los datos personales.

Un ejemplo de aquellos mecanismos implementados por las empresas con el fin de mejorar sus sistemas de tratamientos de datos es aquella que surgió en 2016, Barrios explica que "la Asociación para la IA -la Partnership on Artificial Inteligence- surgió en beneficio de las personas y la sociedad con el fin de "estudiar y formular las mejores prácticas sobre las tecnologías de la IA, las empresas que hacen parte de esa asociación son Amazon, Apple, Google, Facebook, IBM y Microsoft. Así mismo, DeepMind, una de las compañías líderes mundial de IA, adquirida por Google en 2014, presentó un nuevo comité de ética "para ayudar a los tecnólogos a poner en práctica la ética y para ayudar a la sociedad a anticipar y dirigir el impacto de la IA de manera que trabaje para el beneficio de todos"[111].

[110] Reglamento (EU) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. Pág. 2. Consultado el 18 d enero de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

[111] Cit. por Martínez Devia, Andrea. 2019. La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? Revista La Propiedad Inmaterial. 27 (jun. 2019), pág. 18. Consultado el 30 de enero de 2023. Disponible en: https://revistas.uexternado.edu.co/index.php/propin/article/view/6071/7789

Cuando las empresas implementan programas como los descritos anteriormente, aumentan la confianza de sus clientes y/o usuarios; y acompañados de una eficiente política empresarial y práctica de las leyes nacionales e internacionales, auguran un mejor y seguro tratamiento de los datos personales. Esto, además, trae consigo un crecimiento de la economía digital, un aumento del mercado y de la competitividad. Junto a ello, se brinda mayor confianza a las personas para una constante innovación de las tecnologías de la información (TIC'S), la internet y de la inteligencia artificial.

No todo está en manos de las empresas y gobiernos, es además un constante trabajo con toda la misma sociedad, la cual, debe mantenerse informada y actualizada sobre prácticas que beneficien a su relación con las TIC'S, la internet y la IA. Para ello, Martínez hace algunas recomendaciones para proteger nuestros datos personales:

I. "limitar los datos que se publican, no se deben compartir datos como dirección, datos personales, bancarios, número telefónicos o domicilios.
II. uso limitado de mensajes privados, es decir, no compartir contraseñas, datos bancarios y ninguna información comprometedora, ya que dichos mensajes además de captar información pueden ser objeto de *phishing*[112].
III. borrar el historial de búsqueda del navegador.
IV. utilizar la navegación incógnita para que herramientas como las cookies no puedan identificar a la persona.
V. uso de contraseñas seguras.
VI. uso de redes de wifi privadas.

[112] Microsoft, define *phishing* como un ataque que intenta robar su dinero o identidad, haciendo que divulgue información personal (como número de tarjeta de crédito, información bancaria, o contraseñas) en sitios web que fingen ser sitios legítimos. Los delincuentes suelen finger ser empresas prestigiosas, amigos o conocidos en un mensaje falso, que contiene un vínculo a un sitio web de phishing. Microsoft. Protéjase de phishing. Consultado el 30 de enero de 2023. Disponible en: https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

VII. leer los términos y condiciones de las plataformas y redes sociales a las que se adhieren”[113].

Dado que los avances tecnológicos acontecen muy rápido y no espera a que los humanos terminen de adaptarse, las personas deben de estar preparadas para convertirse en auténticos y activos conocedores de las plataformas que visitan, de las redes que usan, de los servicios o productos que compran en internet. En general, de su actuar con la internet y la IA. Esto con el objetivo de que sepan cómo sacar el mayor provecho a estas herramientas digitales, pero también para prevenirse de posibles desventajas por su uso. De igual manera, es importante que las personas sepan cuales son los mecanismos legales que se pueden usar para prevenir o contrarrestar alguna vulneración a su vida privada y a sus derechos humanos.

2.2 Uso para fines políticos

a) El análisis de los datos personales para preferencias políticas, estrategia y fraude electoral

Una constante de la tecnología es que siempre se innova, y es precisamente esa innovación por la que los seres humanos aprovechamos de ella para mejorar nuestros hábitos, nuestro trabajo, nuestra manera de relacionarnos, y claro, también de hacer política.

Los datos personales se usan desde hace años para diversas actividades, algunas de ellas fue la manera de hacer política. Pero antes de explicar cómo los datos personales se usan para predecir, modificar, o inducir cambios de comportamiento en los electores, es necesario explicar poco a poco cómo se fue desarrollando esta práctica.

Para que los políticos y los partidos mejoraran su visibilidad y así aumentaran su número de simpatizantes, se necesitaba innovar la manera en la que se hacía política. La personalización de la política surge ante esa necesidad de aumentar el número de

[113] Martínez Devia, Andrea. 2019. La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales?. Revista La Propiedad Inmaterial. 27 (jun. 2019), pág. 18. Consultado el 30 de enero de 2023. Disponible en: https://revistas.uexternado.edu.co/index.php/propin/article/view/6071/7789

partidarios. De acuerdo con Rebolledo, “la personalización de la política consta de tres componentes: la visibilidad del líder o candidato con respecto al grupo político; las características personales -en referencia a cualquier rasgo de la personalidad, sin distinguir entre características políticas y no políticas-; y aspectos de la vida privada del político. Así mismo, la personalización de la política puede analizarse desde el sistema de los medios, el sistema político y el electorado”[114]. Estos tres últimos elementos son los que le dan forma a la actividad política. Por un lado, el sistema político abarca la forma en la que los actores políticos son expuestos por sus partidos, así como las estrategias usadas para exponer al político. En cuanto al electorado, que se ve directamente influenciado por el sistema de los medios (cubierto por medios tradicionales o modernos), se relaciona en la forma en el ciudadano percibe al político o grupo político.

La personalización de la política no es un fenómeno nuevo. No es hasta el siglo XX que cambia de contexto para adaptarse a las nuevas formas de comunicación. Y en el siglo XXI, la personalización de la política encuentra la manera de adaptarse a las nuevas tecnologías, además de los nuevos movimientos sociales, tecnológicos, culturales, políticos y económicos.

Con la llegada de las nuevas tecnologías de la información, de la internet y en general del gran uso de los distintos medios de comunicación, provocaron un salto cualitativo en el predominio de la imagen, y con ello, de la persona frente a ideas, conceptos u organizaciones colectivas[115]. Con esto, la actividad política comienza a centrarse en la imagen del candidato, y ya no tanto en los temas de la agenda política.

Una vez que se comienza a hacer uso de las redes sociales y plataformas digitales, los datos de las personas se convierten en un activo de mucho valor no sólo para las empresas, también para los políticos. Es por ello por lo que los grupos políticos parecen estar más atentos y preocupados por ganar más simpatizantes a través de masivos mensajes en internet y en medios tradicionales de comunicación, los cuales tratan acerca de la imagen del o la candidata, que de velar objetivamente por crear soluciones efectivas

[114] Rebolledo, Marta. 2017. La personalización de la política: una propuesta de definición para su estudio sistemático. Revista de comunicación. ISSN: 1684- 0933. Consultado el 02 de febrero de 2023. Disponible en: https://revistadecomunicacion.com/es/articulos/2017_2/7_Art.html
[115] *Ibidem*.

para los problemas que acontecen en un Estado, país o territorio. Por esta razón es que Schwartzenberg escribía: “en otros tiempos, la política eran las ideas. Hoy son las personas. O más bien los personajes”[116].

Una vez entendido como los procesos políticos y la manera de hacer política fue cambiando a través de la personalización de la política, es necesario entender cómo con la ayuda de la tecnología se logra que ciertos candidatos obtengan más ventaja sobre otros para ocupar el poder. Un interesante estudio de Kruikemeier señala que “el potencial de internet de conectar con los votantes y movilizarlos, les da a los políticos la oportunidad de promoverse a ellos mismos y comunicar interactivamente con el electorado, sin la interferencia de los periodistas”[117]. Por eso, si las campañas tradicionales ya no se basan tanto en las franjas televisivas y radiales, así como en el “puerta a puerta”; hoy en día se trata de distinguir nichos y encapsular la oferta política en formatos que circulan a gran velocidad: tuits, vídeos, imágenes, correos electrónicos, mensajes de texto, memes, etc. Se trata entonces de cualquier canal que permita a los candidatos exponer su vida privada para mostrar cercanía, circular una frase célebre, o emplazar a otro candidato con el fin de atraer, sino votantes, al menos “seguidores”[118].

Las técnicas usadas para recopilar, tratar y analizar la información obtenida por los datos personales son diversas. La importancia de entender estas técnicas y saber cómo proteger a las personas ante posibles fraudes o menoscabo en su vida privada, es muy importante para el ámbito del derecho. Por ejemplo, González explica que:

> *“Gran parte de los datos sobre redes digitales o internet se obtienen a partir de métodos de programación mediante los cuales se automatiza la recolección de información de sitios web, periódicos o redes sociales, una técnica conocida como “web scraping”. Twitter, por ejemplo, ha desarrollado y puesto a disposición del público un código que sirve como*

[116] Cit. Por Rebolledo, Marta. 2017. La personalización de la política: una propuesta de definición para su estudio sistemático. Revista de comunicación. ISSN: 1684- 0933. Consultado el 02 de febrero de 2023. Disponible en: https://revistadecomunicacion.com/es/articulos/2017_2/7_Art.html

[117] Kruikemeier, S. 2014. How political candidates use Twitter and the impacto on votes. Computers in Human Behavior 43: 131-139.

[118] González, Felipe. 2019. Big data, algoritmos y política: las ciencias sociales en la era de las redes digitales. Cinta de moebio, núm. 65, abril-septiembre, pp. 267-280. Consultado el 02 de febrero de 2023. Disponible en: https://www.redalyc.org/journal/101/10160628010/

vía de acceso a la información que se produce públicamente en la red, a través de los que se conoce como "Application Programming Interface" o API. Esto explica por qué una parte importante de la investigación empírica en este campo se base en datos recogidos de dicha red (pues no es el caso de Facebook, que tiene políticas de privacidad que impiden extraer información de cuentas que no sean públicas). En este sentido, los investigadores quedan a merced de las empresas que sirven de intermediarios, en la medida en que estas deben poner la información a disposición, muchas veces de manera limitada"[119].

Hoy en día la sobre exposición de contenidos en las redes sociales, hace que surja un fenómeno nuevo, y es que con la llegada de los *influencers*[120], los políticos comienzan a ver otras formas de conseguir partidarios, lo cual, con modelos de inteligencia artificial resulta muy sencillo micro-segmentar y aún los *influencers* con audiencias pequeñas son rentables porque se pueden sumar sectores de pequeña escala a movimientos, narrativas, contenidos y descripciones sin orientación electoral o política que vayan sembrando actitudes, datos y detalles considerados útiles o claves a la hora de votar[121]. De acuerdo con el 18º Estudio sobre los Hábitos de Personas Usuarias de Internet en México 2022, la política ocupa en 9º lugar de los temas de interés en la red social TikTok en hombre y mujeres[122]. De ese estudio se desprende que la gente de entre 35 y 44 años, son aquellas las que prefieren ver temas de política en TikTok, los algoritmos de esta red social hacen que se compartan los vídeos y publicaciones de sus intereses a sus seguidores (de más o menor edad). Así mismo, aquel partido o grupo políticos que

[119] Gonzáles, F. 2019. Big Data, algoritmos y política: las ciencias sociales en la era de las redes digitales. Cinta moebio. Consultado el 07 de febrero de 2023. Disponible en: https://www.redalyc.org/journal/101/10160628010/

[120] De acuerdo con Hosteltur un *influencer* "es una persona que destaca en una red social u otro canal de comunicación y expresa opiniones sobre un tema concreto que ejercen una gran influencia sobre muchas personas que la conocen". Consultado el 10 de febrero de 2023. Disponible en: https://www.hosteltur.com/comunidad/004455_el-marketing-de-influencers-tambien-ha-llegado-a-los-hoteles.html

[121] Paredes, Alfredo. 2021. Influencers y política 4.0. Forbes. Consultado el: 10 de febrero de 2023. Disponible en: https://www.forbes.com.mx/red-forbes-influencers-y-politica-4-0/

[122] Asociación de Internet MX. 18º Encuesta 18º Estudio sobre los Hábitos de Personas Usuarias de Internet en México 2022. Consultado el 10 de febrero de 2023. Disponible: https://irp.cdn-website.com/81280eda/files/uploaded/18%C2%B0%20Estudio%20sobre%20los%20Habitos%20de%20Personas%20Usuarias%20de%20Internet%20en%20Mexico%202022%20%28Socios%29%20v2.pdf

mejor sepa cómo usar estas redes sociales, es quien lograr encontrar una mayor ventaja sobre el resto de sus contrincantes políticos.

b) El caso Trump, Facebook y Cambridge Analytica

Un interesante ejemplo sobre el uso de los datos de millones de personas para la actividad política la constituye el caso de las elecciones de Estados Unidos de América, en la que Donald Trump usaría principalmente Facebook y Twitter para conseguir ventaja contra la candidata Hillary Clinton y así convertirse en presidente de los Estados Unidos de América en 2017. La diferencia de otros candidatos a la presidencia de Norteamérica y Trump fue que él decidió apostar astuta y estratégicamente en las redes sociales, y no tanto por los medios de difusión tradicionales, para difundir la mayor parte de su candidatura, de hacerse de más partidarios e incluso de hacer que las personas con probabilidad de votar por Hillary Clinton dejaran de serlo. Desde inicios de la campaña, su director digital hizo ver a Donald Trump que no merecía la pena malgastar dinero en anuncios en televisión, medio en el que el candidato ya tenía gran repercusión gracias a sus explosivas declaraciones[123]. En su lugar, su equipo digital decidió apostar por las redes sociales y el Big Data, en este tenor, Cellan-Jones muestra cuantitativamente el poder que en este caso la red social Facebook tenía en ese entonces en la población estadounidense:

> *"Alrededor de unos 156 millones de estadounidenses tienen cuentas en Facebook y, según un estudio reciente, dos tercios obtienen sus noticias allí. Es entonces cuando entra en juego la idea de una burbuja que filtra la información: quienes se inclinan por Trump sólo verán noticias que reflejan su visión del mundo y lo mismo le ocurrirá a quienes tiene un pensamiento liberal. El algoritmo que selecciona las noticias que muestra la red sólo ofrece aquellas informaciones que tú*

[123] Rodríguez-Andrés, Roberto. 2018. Trump 2016: ¿presidente gracias a las redes sociales? Palabra clave. Consultado el 08 de enero de 2023. Disponible en: https://palabraclave.unisabana.edu.co/index.php/palabraclave/article/view/8170/pdf

y tus amigos quieren creer y no realiza una verificación de los datos que contiene"[124]*.*

Unos de los principales componentes a nivel digital y de redes sociales fue el trabajo realizado por la empresa Cambridge Analytica hacia Donald Trump, la cual, extrajo información privada de los perfiles de Facebook de más de 50 millones de usuarios sin su consentimiento, esto de acuerdo con declaraciones de exempleados, exasociados y documentos de Cambridge Analytica, lo cual dio como resultado a una de las filtraciones más grandes de la historia de las redes sociales[125]. Fue así como la campaña de Trump, consciente del poder de Facebook, utilizó dicha red social con tres objetivos principales: recaudar fondos a través de pequeñas donaciones (alcanzando los USD 250 millones por esta vía), difundir mensajes a públicos prioritarios a través del *microtargeting* que permite esta red social (como los destinados a la *voter suprpression* de votantes de Clinton) y diseminar noticias[126].

c) Para entender el papel del *big data*

En lo que a los datos personales respecta, Parscale, quien fuera asesor digital para la campaña presidencial de Donald Trump, convenció al candidato para apostar por el Big Data en las redes sociales. Como explica Abdullin, fue así como "comenzaron a trabajar en encuestas *online*, llamadas telefónicas, y *big data* para conocer mejor a los electores, utilizando esta información para recaudar fondos y centrar mensajes y publicidad en los medios prioritarios y en lugares y electores clave (sobre todo los blancos descontentos con la política tradicional)"[127].

[124] Cellan-Jones, Rory. Elecciones en Estados Unidos: ¿fue Facebook la clave para el triunfo de Donald Trump? BBC NEWS MUNDO. Consultado el: 08 de febrero de 2023. Disponible en: https://www.bbc.com/mundo/noticias-internacional-37946548

[125] Rosenber, M., Confessore, N. y Cadwalladr, C. (2018). La empresa que explotó millones de datos de usuarios de Facebook. The New York Times. Consultado el 08 de febrero de 2023. Disponible en: https://www.nytimes.com/es/2018/03/20/espanol/cambridge-analytica-facebook.html

[126] Rodríguez-Andrés, Roberto. 2018. Trump 2016: ¿presidente gracias a las redes sociales? Palabra clave. Consultado el 08 de enero de 2023. Disponible en: https://palabraclave.unisabana.edu.co/index.php/palabraclave/article/view/8170/pdf

[127] Cit. Rodríguez-Andrés, Roberto. 2018. Trump 2016: ¿presidente gracias a las redes sociales? Palabra clave. Consultado el 08 de enero de 2023. Disponible en: https://palabraclave.unisabana.edu.co/index.php/palabraclave/article/view/8170/pdff

Data Analythis y los asesores digitales de Trump usaron diversas técnicas para mejorar su presencia en las redes sociales y sacarle el mejor provecho de ellas. Aunque fueron diversas las técnicas que se usaron para influir en los estadounidenses, y hacer que sintieran simpatía y votaran por él, las maneras más controversiales fueron aquellas en las que Data Analythis, usando Facebook, hicieron que se difundieran noticias falsas, en las cuales muchas de ellas, desfavorecía a su contrincante, Hillary Clinton.

Con la llegada de la cuarta revolución industrial, en siglo XXI, el uso del Big Data, de la Inteligencia Artificial, del internet de las cosas, la ciencia de datos, y la realidad virtual se hace necesario el estudio profundo de las situaciones que se presentan día con día con estas áreas de estudio. Desafortunadamente, el derecho no puede seguir el ritmo de la tecnología, sin embrago, los esfuerzos por parte de los legisladores, administradores de justicia, y de los estudiosos del derecho en cuanto a la regulación y entendimiento de las situaciones jurídicas relacionadas con la tecnología, siempre son necesarios. México, por un lado, necesita estudiar y entender mejor cómo funcionan y se pueden regular estas nuevas prácticas que involucran el uso de cualquier tipo de tecnología y el internet.

2.3 Los datos personales y su relación con la inteligencia artificial.

El impacto de las nuevas tecnologías sobre nuestros datos personas son cada vez más sorprendentes. El ser humano, en su deseo de siempre descubrir y experimentar, ya no sólo usa su información para acceder a servicios, plataformas, aplicaciones o adquirir bienes, ahora, desea que la vida en general sea cada vez más sencilla, y una de estas formas de hacerlo posible es a través de la inteligencia artificial.

El origen de la Inteligencia artificial comienza con la llegada de la 4º revolución industrial. Por su parte, Martínez, define a la Inteligencia Artificial (IA) como:

> "*la simulación realizada por máquinas o sistemas informáticos de procesos o de actividades realizadas por la inteligencia humana. El funcionamiento de la IA se basa en el análisis de miles de datos conocidos como big data, dentro de los que se pueden encontrar datos de carácter personal, los cuales, por su esencia deben de ser*

tratados de manera ética, responsable y transparente para proteger los derechos de los titulares"[128].

Por su parte, Corvalán, precisa que "la IA se sustenta en algoritmos inteligentes o en algoritmos de aprendizaje que, entre muchos otros fines, se utilizan para identificar tendencias económicas, predecir delitos, diagnosticar enfermedades, predecir nuestros comportamientos digitales, etc"[129]. De acuerdo con Domingos, un algoritmo puede ser definido como un "conjunto preciso de instrucciones o reglas, o como una serie metódica de pasos que puede utilizarse para hacer cálculos, resolver problemas y tomar decisiones. El algoritmo es la fórmula que se emplea para hacer un cálculo"[130].

Si bien es cierto que la IA puede simular procesos o actividades humanas, esta misma también es capaz de analizar, aprender, planificar y ejecutar por sí misma. Dada esta idea de la IA, es importante que la sociedad, y sobre todo los gobiernos, actualicen su normativa para una mejor creación de máquinas y programas súper inteligentes. Replantea, además, que los creadores de esta IA sean personas libres de prejuicios, con una fuerte base en cuando a la ética y responsabilidad del programador y de la IA.

Debido al creciente aumento de teléfonos inteligentes, redes sociales, plataformas y aplicaciones, los datos de las personas se encuentran en manos de las empresas, gobiernos y asociaciones, los cuales, muchas veces no son conscientes de la importancia que tiene tratar adecuadamente muchos datos. De acuerdo con Garriga, "la implementación de algoritmos y estadísticas en la IA se pueden obtener resultados concretos como el comportamiento de las personas, sus gustos, la toma de decisiones, el reconocimiento de voz, la situación económica, la salud, los intereses, entre otros datos que se utilizan con diversos fines, y se encuentran al alcance de empresas,

[128] Martínez Devia, A. "La inteligencia artificial, el Big Data y la era digital: ¿una amenaza para los datos personales?", Revista La Propiedad Inmaterial no. 27, Universidad Externado de Colombia, enero-junio 2019, pp.5-23. DOI: https://doi.org/10.18601/16571959.n27.01

[129] Corvalán, Juan. Inteligencia artificial: retos, desafíos y oportunidades – Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia. ARTIGOS. Rev. Investig. Const. 5 (1). Enero-abril 2018. Consultado el 20 de enero de 2023. Disponible en: https://www.scielo.br/j/rinc/a/gCXJghPTyFXt9rfxH6Pw99C/?lang=es

[130] Cit. Por Corvalán, Juan. Inteligencia artificial: retos, desafíos y oportunidades – Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia. ARTIGOS. Rev. Investig. Const. 5 (1) • Jan-Apr 2018. Consultado el 20 de enero de 2023. Disponible en: https://www.scielo.br/j/rinc/a/gCXJghPTyFXt9rfxH6Pw99C/?lang=es

Estados e incluso particulares[131]. Esto presenta un área de interés para gobiernos, empresas y sociedad en general. Por ello, ya no sólo es necesario estudiosos que se dediquen al análisis de estos escenarios, requiere además que exista voluntad por parte de los legisladores para implementar y mantener actualizados los marcos normativos. Incluso, se requiere de las personas un mayor interés para exigir protección a sus datos personales y a su privacidad. Lo anterior se logra cuando existe una sociedad que se mantenga informada e interesada sobre lo que se hace con sus datos personales.

a) La inteligencia artificial en la vida cotidiana y sus riesgos

La inteligencia artificial está presente en nuestras vidas desde hace algunos años. Con el uso de las cada vez más modernas tecnologías de la información, estás se vuelven, con el pasar de los días, parte de nuestra vida.

La IA no sólo son robots súper inteligentes, ni carros autónomos, casas domóticas o tecnología de punta que poca gente puede ver o tener. La inteligencia artificial la encontramos en los algoritmos de las redes sociales, plataformas, y aplicaciones que usamos; de los sitios web que visitamos; de los relojes, bocinas, pantallas, computadoras y teléfonos inteligentes que cada vez más gente desea usar, entre otros. A pesar de que los seres humanos usamos estas tecnologías, muy poca gente es consciente de sus efectos y desventajas.

A nivel mundial, se observan algunos casos que ejemplifican algunos de los riesgos que existen por el mal tratamiento de los datos personales y la IA. Por ejemplo, Joy Boulamwini, investigadora informática, fue una de las primeras en descubrir que los sistemas de inteligencia artificial pueden ser racistas. Su historia, por ejemplo, fue documentada a través del film *Coded Bias* en 2020. La película explica como el sistema de reconocimiento de cara puede fallar en función del color de la piel. La mayoría de los algoritmos que se esconden detrás de la IA, fueron desarrollados por hombre blancos, lo cual prevalece su visión del mundo, creando un trato discriminatorio hacia personas diferentes. Los algoritmos están codificados para identificar principalmente rostros

[131] Cit. por Martínez Devia, A. “La inteligencia artificial, el Big Data y la era digital: ¿una amenaza para los datos personales?”, Revista La Propiedad Inmaterial no. 27, Universidad Externado de Colombia, enero-junio 2019, pp.5-23. DOI: https://doi.org/10.18601/16571959.n27.01

occidentales, de ahí que, por ejemplo, la IA tenga problema con otros colores de piel[132]. Por ello, es importante que los algoritmos sean actualizados constantemente, además de que contenga una mayor diversidad de datos.

No sólo es necesario que la información para alimentar a los algoritmos sea más diversa, también implica que las mismas corporaciones, los altos directivos, y las altas autoridades tanto del sector privado como del sector público, tengan la voluntad de hacer a estos sistemas inteligentes más justos, equitativos e incluyentes.

De modo similar, en algunos países como en China, el gobierno y las empresas hacen uso desmedido de la captación de datos personales, muchas veces, a través de cámaras de vigilancia. Los expertos en vigilancia digital de Estados Unidos descubrieron que la multinacional HUAWEI participó, junto con el gobierno chino, en el desarrollo de la llamada “alarma Uigur”. Se supone que este software de reconocimiento facial puede identificar en segundos a personas de la minoría musulmana de los uigures[133], pero a pesar de que esta tecnología aún comete errores para asociar objetos con otras imágenes, lo sorprendente es que aun así se usa esa tecnología en el país asiático. El problema de esto radica en que cuando una persona es considerada como uigur, esta es detenida arbitrariamente en manos de la policía de China, sin el respeto a los derechos humanos. Además, el gobierno somete a este grupo minoritario, y a cualquier persona considerada como uigur, a una reeducación contra su voluntad en campos de internamiento, en los cuales, de acuerdo con China, estos tienen el propósito de combatir el terrorismo extremo y el extremismo religioso[134]. Sin embargo, de acuerdo con el Comité de la ONU para la Eliminación de la Discriminación Racial, existen muchas dudas sobre el sistema de reeducación hacia los uigures, además de que crece la preocupación

[132] López, Pablo y Gómez, Juan [productores]. ¿Cómo discrimina la inteligencia artificial? ¿quienes son sus víctimas? (2021). DW Español. Consultado el 20 de enero de 2023. Disponible en: https://www.youtube.com/watch?v=mWGzicjqAc0
[133] *Ibidem*.
[134] BBC News mundo. Uigures en China: los motivos por los que China detiene a los miembros de esta minoría musulmana. 2020. Consultado el 20 de enero de 2023. Disponible en: https://www.bbc.com/mundo/noticias-51531714

internacional por las desapariciones a gran escala que se producen en los campos de reeducación[135].

b) Legislación sobre la inteligencia artificial

En México, por ejemplo, no existe una regulación específica sobre la IA. Fue en 2010 cuando México publicó en el Diario Oficial de la Federación la primera ley que obligaba a los particulares un "correcto y adecuado" uso de los datos personales, fue así como nace la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y desde entonces, no existe una actualización de dicha ley. Si bien es cierto existió voluntad para proteger los datos personales, no existe la voluntad para mantenerla actualizada dicha ley. Además, cuando se decretó esta ley, no se vislumbraba por parte de los legisladores la prevención de futuras situaciones que pudiesen afectar los derechos humanos de los titulares de los datos personales. Se requiere necesariamente una mejora a los sistemas normativos que obligan a particulares y gobiernos, tener un límite en cuanto al uso de la IA, y del tratamiento de los datos personales.

Tan sólo en México de 2010 a 2023, surgieron diversos y muy importantes cambios en el ámbito de las nuevas tecnologías. También, se observa un incremento considerable sobre el uso de las nuevas tecnologías en la población mexicana. De acuerdo con la Asociación de Internet MX, desde 2015 hasta 2021, existe un incremento del 18.2% en cuanto a la representación de la población de 6 años o más en México[136], que se considera internauta. De lo anterior, se concluye que, hasta el día de hoy, existen 88.6 millones de personas (mayores de 6 años), y que representa el 75.6% de la población[137], que usa y navega en la red digital.

México puede tomar como inspiración y guía diversas leyes referentes en la materia de otros países, por ejemplo, España junto con su Secretaría de Estado de Digitalización e

---

[135] BBC news mundo. Quiénes son los uigures, la etnia que China está deteniendo en "campos de reeducación". 2018. Consultado el 20 de enero de 2023. Disponible en: https://www.bbc.com/mundo/noticias-internacional-45368245

[136] Asociación de Internet Mx. 18º Estudio sobre los hábitos de Personas Usuarias de Internet en México 2022. Mayo 2022. Pág. 8. Consultado el 18 de enero de 2023. Disponible en: https://irp.cdn-website.com/81280eda/files/uploaded/18%C2%B0%20Estudio%20sobre%20los%20Habitos%20de%20Personas%20Usuarias%20de%20Internet%20en%20Mexico%202022%20%28Socios%29%20v2.pdf

[137] *Ibidem*.

Inteligencia Artificial, realizó la Carta de los Derechos Digitales en 2021. Por su parte, la Unión Europea creó en 2018 el Reglamento General de la Unión Europea de Protección de Datos Personales (RGDP) en el cual se ofrecen bases, principios y alternativas a posibles situaciones que se pueden presentar por uso inadecuado de los datos personales y sobre el rápido avance de las tecnologías. Otro documento expedido por la Unión Europea y que contempla la relación de la IA, los datos personales y las nuevas tecnologías es "El Proyecto de Guía ética para el Uso Responsable de la Inteligencia Artificial", el cual, algunos de los puntos más importantes son:

- "Un enfoque de la IA centrado en los seres humanos.
- Garantizar el fin ético de la IA.
- La especial atención a los grupos vulnerables, como son los menores de edad o las personas con discapacidades.
- El respeto por los derechos fundamentales de los titulares.
- Los principios de transparencia, privacidad y seguridad de los datos personales.
- La importancia de la libertad humana"[138].

A pesar de que las principales compañías creadoras de IA provienen de Estados Unidos de América, Europa y Asia, es importante que los legisladores mexicanos adopten medidas que garanticen la protección de los derechos humanos y digitales de las personas en México. Un primer punto es que, con la llegada de las compañías extranjeras a México, éstas respeten los lineamientos básicos de protección de derechos humanos y de protección de datos personales, además, que las mismas estén en constante auditoría. Otro punto que depende en gran medida del gobierno es que estos garanticen la correcta aplicación de la ley, evitando así actos de corrupción.

Como señaló el vicepresidente para la Agenda Digital del Ejecutivo Comunitario, Andrus Ansip, "para que la gente acepte y utilice sistemas basados en inteligencia artificial

[138] Martínez Devia, A. "La inteligencia artificial, el Big Data y la era digital: ¿una amenaza para los datos personales?", Revista La Propiedad Inmaterial no. 27, Universidad Externado de Colombia, enero-junio 2019, pp.5-23. Consultado el 19 de enero de 2023. Disponible en: https://doi.org/10.18601/16571959.n27.01

necesita confiar en ellos, saber que su privacidad es respetada, que las decisiones no son parciales”[139].

2.4 Los datos personales y su uso para fines delictivos

Fue a partir del siglo XXI cuando los delitos informáticos fueron en aumento, esto debido al gran avance, rápida difusión y el exponencial uso de las nuevas tecnologías de la información entre todas las edades posibles en el mundo. Además, la forma en que se cometían estos delitos fueron diferentes y con distintos grados de dificultad que se presentaba en el momento. Antes no se pensaba que la internet podría ser un espacio peligroso, ahora, se puede observar distintas ventajas y desventajas que ofrece esta moderna herramienta; el cual, en el peor de los casos, representa una amenaza potencial para la seguridad de un país o de toda una comunidad.

Por una parte, el ciberespacio se convirtió en el nuevo terreno de guerra y de delitos, por ello, es importante comenzar por definir qué es ciberespacio. El ciberespacio puede entenderse como “la red”, es el nuevo medio de comunicación que emerge de la interconexión mundial de los ordenadores, designa también el oceánico universo de informaciones que contiene, así como los seres humanos que navegan en él y lo alimentan[140]. En este sentido, Curtis argumenta que “el ciberespacio es un dominio artificial construido por el hombre, diferenciado de los otros cuatro dominios de guerra (tierra, aire, mar y espacio); aunque se haya formalizado recientemente, el ciberespacio puede afectar a las actividades en los otros dominios y viceversa”[141]. Además, el ciberespacio está profundamente vinculado y apoyado por medios físicos, por ejemplo, las redes eléctricas. Si se ataca a esta interconexión puede tener repercusiones graves sobre las estrategias de seguridad, nacionales e internacionales[142]. Esta nueva forma de

---

[139] *Idem*.

[140] Sierra Gutiérrez, Luis Ignacio. (2009). La cultura en la era del ciberespacio: Cibercultura. La cultura de la sociedad digital. *Signo y Pensamiento*, *28*(54), 382-398. Consultado el 1 de marzo de 2023. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-48232009000100029&lng=en&tlng=es

[141] Cit. Por Pons Gamón, Vicente. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad URVIO, Revista Latinoamericana de Estadios de Seguridad, núm. 20, 2017, pp. 80-93. Consultado el 01 de marzo de 2023. Disponible en: https://www.redalyc.org/journal/5526/552656641007/

[142] Pons Gamón, Vicente. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad URVIO, Revista Latinoamericana de Estadios de Seguridad, núm. 20, 2017, pp. 80-93. Consultado el 01 de marzo de 2023. Disponible en: https://www.redalyc.org/journal/5526/552656641007/

ataque aumentó durante los últimos años, principalmente en países desarrollados y semidesarrollados, esto debido a que los delitos se cometen fácilmente; desde cualquier parte del mundo sin estar presente el atacante en el país que planea vulnerar; se requieren escasos recursos humanos; y no siempre se terminan castigando estas vulneraciones, entre algunas otras razones es porque el país atacado no cuenta con la regulación adecuada para castigar el delito, dado que no se cuenta con el personal humano capacitado para hacer frente a estos ataques, o porque requiere de una gran inversión que, en la mayoría de los casos, no se tiene contemplada; entre otros.

En México, unos de los problemas es que los registros relacionados con ciberataques están muy por debajo de los datos que aportan organismos y empresas especializadas en el sector[143]. Nuestro país, se ha convertido en uno de los países de América Latina con mayor número de ciberataques[144], esto por diversas razones, algunas de ellas porque México logró un crecimiento económico a lo largo de las últimas décadas, lo cual la convierte en un país atractivo para los delincuentes en el ciberespacio; porque crece el mercado del sector financiero, y con ello su número de clientes; y también el número de usuarios del internet es exponencial, lo cual trae consigo mayor uso de redes sociales, de compras por internet y en general, las personas confían tanto en la red, que ingresan un sinfín de datos personales en casi cualquier aplicación, plataforma o servicio de internet. Corona Nakamura declaró que, “según información del FBI de Estados Unidos, México es uno de los que más ataques cibernéticos registró a nivel mundial durante 2020”[145]. En México, tras la pandemia de COVID-19, hubo un crecimiento en delitos cibernéticos que pasaron de apenas 300.3 millones en el 2019 a 12 mil millones de intentos en el 2021, un crecimiento casi 400 veces, lo que convirtió al país en el más

[143] Calderón, Christopher. México “clientazo” de los ciberataques: crecen 42% amenazas por internet. El Financiero. Consultado el 2 de marzo de 2023. Disponible en: https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/

[144] De acuerdo con IBM, los ciberataques son intentos no deseados de robar, exponer, alterar, deshabilitar o destruir información mediante el acceso no autorizado a los sistemas informáticos. Consultado el 02 de marzo de 2023. Disponible en: https://www.ibm.com/mx-es/topics/cyber-attack

[145] BUSINESS INSIDER MÉXICO Los delitos cibernéticos en México podrán ser tema de Seguridad Nacional en México. Consultado el 02 de marzo de 2023. Disponible en: https://businessinsider.mx/delitos-ciberneticos-mexico-considerados-tema-seguridad-nacional_tecnologia/#:~:text=De%20acuerdo%20con%20la%20Condusef,y%20banca%20m%C3%B3vil%20cada%20hora.

atacado en América Latina[146]. Este gran aumento en parte se debe a que casi todas las empresas, gobierno, escuelas y sociedad en general decidió realizar la mayoría de sus actividades desde la virtualidad. En este sentido, Ramón Castillo, especialista en Seguridad de la Información de Forcepoint, una empresa que ofrece seguridad cibernética, menciona que "a raíz de la pandemia crecieron significativamente los ataques de ingeniería social, particularmente ataques de *phishing,* y *malware*, es decir, que los hackers[147] se enfocaron en atacar las redes de los usuarios finales, lo que derivó en un incremento de hasta 300 por ciento en ciberataques, de los cuales, más del 60 por ciento estuvieron dirigidos a ataques de banca en línea"[148].

Para entender mejor la gravedad de algunas de anteriores cifras, es conveniente explicar cuáles son los delitos cibernéticos más usuales en la era digital y cómo estos dañan no sólo el patrimonio de las personas, en el peor de los casos, su integridad y su vida.

Por lo que se refiere a ciberataques más habituales, IBM apunta que son:

- *"Troyano de puerta trasera: un troyano de puerta trasera crea una vulnerabilidad de puerta trasera en el sistema de la víctima, lo que permite al atacante obtener un control remoto y casi total. Usado con frecuencia para vincular las computadoras de un grupo de víctimas a una botnet o red zombi, los atacantes pueden usar el troyano para otros delitos cibernéticos.*
- *Malware: el malware es sotfware malintencionado que puede inutilizar los sistemas infectados. La mayoría de las variantes de malware destruyen datos al eliminar o limpiar archivos críticos para la capacidad de ejecución del sistema operativo.*

[146] Calderón, Christopher. México "clientazo" de los ciberataques: crecen 42% amenazas por internet. El Financiero. Consultado el 2 de marzo de 2023. Disponible en: https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/

[147] De acuerdo con Pichincha, un *hacker* son personas expertas que poseen conocimientos informáticos avanzados para acceder a un determinado sistema o dispositivo y realizar modificaciones desde adentro, principalmente destinadas a la seguridad informática y al desarrollo de técnicas para su mejora. Consultado el 7 de marzo de 2023. Disponible en: https://www.pichincha.com/portal/blog/post/que-es-un-hacker

[148] Calderón, Christopher. México "clientazo" de los ciberataques: crecen 42% amenazas por internet. El Financiero. Consultado el 2 de marzo de 2023. Disponible en: https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/

- *Phishing: las estafas de phishing intentan robar las credenciales o los datos confidenciales de los usuarios como, por ejemplo, números de tarjetas de crédito. En este caso, los estafadores envían a los usuarios e-mails o mensajes de texto diseñados para que parezcan que proviene de una fuente legítima, utilizando hipervínculos falsos.*
- *Ransomware: el ransomware es un malware sofisticado que se aprovecha de las debilidades del sistema y utiliza un cifrado sólido para mantener los datos o la funcionalidad del sistema como rehenes. Los ciberdelincuentes utilizan ransomware para exigir un pago a cambio de liberar el sistema. Un desarrollo reciente con ransomware es el complemento de tácticas de extorsión.*
- *Ataque de secuencias de comandos entre sitios (XSS): los ataques XSS insertan código malicioso en un sitio web legítimo o en un script de aplicación para obtener información del usuario, a menudo utilizando recursos web de terceros. Los atacantes utilizan con frecuencia JavaScript para ataques XSS, pero también se pueden utilizar Microsoft VCScript, ActiveX y Adobe Flash.*
- *Denegación de servicio (DoS): los ataques DoS y de denegación de servicio distribuida (DDoS) inundan los recursos de un sistema, los abruman e impiden las respuestas a las solicitudes de servicio, lo que reduce la capacidad del sistema para funcionar. A menudo, este ataque es una preparación para otro ataque.*
- *Tunelización de DNS: los ciberdelincuentes utilizan el túnel de DNS, un protocolo transaccional, para intercambiar datos de aplicaciones, como extraer datos de forma silenciosa o establecer un canal de comunicación con un servidor desconocido, como un intercambio de comando y control (C&C).*
- *Inyección de SQL: los ataques de inyección de lenguaje de consulta estructurado (SQL) incorporan un código malicioso en aplicaciones vulnerables, lo que genera resultados de consultas en la base de datos de backend y ejecuta comandos o acciones similares que el usuario no solicitó.*
- *Explotación de día cero: los ataques de explotación de día cero aprovechan las debilidades desconocidas de hardware y software. Estas vulnerabilidades pueden*

existir durante días, meses o años antes de que los desarrolladores se enteren de las fallas"[149]*.*

Estos ejemplos de ciberataque no son los únicos. Sin embrago, son los principales asociados al robo de información privada o de datos personales. No obstante, los ciberdelincuentes usan las "técnicas tradicionales" de delito o ataque también el ciberespacio, o mejor dicho, en la *dark web*. La *dark web* o red oscura se suele definir como una zona no indexable por buscadores convencionales (como Google, Bing, y demás buscadores), y es todo el contenido que se puede encontrar en diferentes *Darknets* (programas o buscadores específicos)[150]. Es importante aclarar que, de acuerdo con Fernández, "la Darknet no es mala por definición. La Darkweb sirve como cobijo a activistas perseguidos en países especialmente férreos con la libertad de expresión, y ayuda a que otros puedan saltarse las censuras locales para acceder a la información"[151].

Una vez entendido en términos generales los tipos de delitos cibernéticos que mayormente se cometen, se dará un panorama general sobre los delitos que acontecieron en México y el mundo dentro del ciberespacio.

De acuerdo con datos de la firma mexicana de ciberseguridad Silikn, tan solo en México, en los primeros seis meses del año 2021, México sufrió 85 mil millones de intentos de ciberataques, que representan más de la mitad de los 120 mil millones de amenazas electrónicas registradas durante todo el año 2020[152]. El aumento del fraude cibernético parece estar íntimamente relacionado con las estafas de compras en comercio electrónico; tan solo de enero a marzo de 2018, estos aumentaron a razón de 74% con

[149] IBM. ¿Qué es un ataque cibernético? Consultado el 3 de marzo de 2023. Disponible: https://www.ibm.com/mx-es/topics/cyber-attack

[150] Cfr. en Fernández, Yúbal. 2021. Qué es la Dark Web, en que se diferencia de la Deep Web y cómo puedes navegar por ella. Xataka Basics. Consultado el 6 de marzo de 2023. Disponible en: https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedes-navegar-ella

[151] *Ibidem.*

[152] Calderón, Christopher. México "clientazo" de los ciberataques: crecen 42% amenazas por internet. El Financiero. Consultado el 2 de marzo de 2023. Disponible en: https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/

relación al mismo periodo del año anterior. Al cierre del primer trimestre de 2018, se reportaban más de un millón de fraudes cibernéticos a nivel nacional, superando por mucho al fraude tradicional, que presentó un total de 659 440 casos en el mismo periodo, según datos de la CONDUSEF[153].

Con respecto a la sensación y cultura de ciberseguridad en la población mexicana, de acuerdo con la encuesta de ciberseguridad de 2022, realizado por la Asociación de Internet MX, el 90.6% de los encuestados refirió que le preocupa la ciberseguridad (este tema se abordará detenidamente en el siguiente apartado). El 22.1% de los usuarios han sido víctimas de alguna vulneración en los últimos 12 meses. De ellos, el 46.5% sufrió algún tipo de fraude o pérdida financiera[154]. Lo que incide en que, de acuerdo con la Dirección General Científica de la Guardia Nacional, desde enero de 2019 hasta abril de 2022, esta atendió más de cinco mil 800 investigaciones por delitos cibernéticos, tales como amenazas, fraude, trata de personas y posesión o distribución de pornografía infantil[155]. Además, del estudio sobre ciberseguridad por parte de la Asociación de Internet MX, el 21.1% de los encuestados mencionan que fueron víctimas de fraude y pérdida financiera (46.5%), suplantación de identidad (27.3%), pérdida de información (22.2%), víctimas de phishing (20.2%), fuga de información sensible (14.1%) y ransomware (8.1%). Todos estos datos muestran el exponencial crecimiento de algunos delitos informáticos tan sólo en México, pero trasladado a un plano más internacional, los ciberdelitos no es lo único que afecta al mundo, también son las ciberguerras y el ciberterrorismo.

Por lo que se refiere a los ciberataques o ciberterrorismo dentro de la dark web, que es un lugar en donde prácticamente cualquiera puede estar en el anonimato, esta profundidad de la web es también un lugar en donde acontecen delitos, como la venta ilegal de drogas, armas, y hasta la venta de datos personales (toda clase de datos, como

[153] Equipo ORCA. 2019. 3 casos reales de delitos informáticos en México. Consultado el 3 de marzo de 2023. Disponible en: https://blog.orcagrc.com/casos-de-delitos-informaticos-en-mexico
[154] Asociación de Internet MX. 2022. Estudio sobre ciberseguridad en empresas, personas usuarias de internet y padres de familia en México. Segunda edición. Consultado el 3 de marzo de 2023. Disponible en: https://irp.cdn-website.com/81280eda/files/uploaded/Encuesta%20Ciberseguridad%202022%20pu%CC%81blica%20230119.pdf
[155] *Ibidem*.

datos de tarjeta de crédito o las contraseñas de cuentas bancarias, plataformas o redes sociales). Es por eso por lo que, de acuerdo con Shulman, experta en ciberseguridad del Instituto Fraunhofer en Alemania, “cualquier persona puede sufrir una vulneración a sus dispositivos electrónicos, bases de datos (en el caso de organizaciones) o a sus cuentas en internet, y que su información o datos personales se vendan en la darkweb para diversos fines, principalmente para cometer fraudes bancarios con sus datos bancarios”[156].

Además, de acuerdo a un testimonio anónimo recabado por la DW Español, la darkweb puede sorprender a cualquier persona por lo fácil que es comprar drogas en internet sin levantar ninguna sospecha, ya que los vendedores usan técnicas muy sofisticadas para seguir manteniéndose en el anonimato[157]. Se estima que el comercio con drogas representa el 62% de todo el mercado de la web oscura. Los países con mayores ingresos por drogas son Alemania, Países Bajos y Reino Unido[158].

En cuanto a la protección de los niños, niñas y adolescentes, las personas encargadas de su cuidado deben proporcionar información elemental para navegar en el ciberespacio de forma segura. Es fundamental para prevenir que ellos sean víctima de *grooming*[159], *sexting*[160] y en general de cualquier tipo de delitos o de personas pedófilas en la internet. Un ejemplo de estos peligros, lo representó ELYSIUM, que fue una plataforma que durante algunos años estuvo funcionando en varios países, pero principalmente en Alemania. Esta plataforma la cual se podía acceder desde la darkweb, los pedófilos compartían vídeos y fotos de abusos sexuales a niños, niñas y adolescentes de todas

[156] Cfr. por Michelle Ostwald. 2021. ¿Están mis datos a la venta en la darkweb? [microdocumental]. Consultado el 7 de marzo de 2023. Disponible en: https://www.youtube.com/watch?v=sMG9UDv6eq8
[157] Cfr. por Michelle Ostwald. 2021. ¿Por qué se venden tantas drogas en la darkweb? [microdocumental]. Consultado el 7 de marzo de 2023. Disponible en: https://www.youtube.com/watch?v=myAFhVbrIlA
[158] *Idem*.
[159] De acuerdo con Save de Children, “*grooming*” es una forma delictiva de acoso que implica a un adulto que se pone en contacto con un niño, niña o adolescente con el fin de ganarse poco a poco su confianza para luego involucrarle en una actividad sexual. Save de Children. 2019. Grooming, qué es, cómo detectarlo y prevenirlo. Consultado el 7 de marzo de 2023. Disponible en: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo
[160] De acuerdo con la UNAM, el “*sexting*” es una práctica la cual involucra el envío de o intercambio de fotografías o vídeos en poses eróticas o de desnudos. UNAM. Sexting, cuidado con tu intimidad. Consultado el 7 de marzo de 2023. Disponible en: https://www.fundacionunam.org.mx/unam-al-dia/sexting-cuidado-con-tu-intimidad/

las edades. Fue hasta 2017 cuando la policía alemana pudo atrapar a los creadores de esa plataforma ilegal y lograron enjuiciarlos y cerrar la plataforma por completo[161].

En cuanto al tema de trata de personas respecta, en Arabia Saudita, existe una aplicación online que facilita la esclavitud moderna. Esta aplicación que actualmente se encuentra disponible en Apple Store y Google Play se llama “Haraj”. La esclavitud moderna ocurre en casi todos los países del mundo y atraviesa líneas étnicas, culturales y religiosas[162]. El término de “esclavitud moderna” en realidad no está definida en la ley, pero en general, se refiere a cualquier forma de trabajo forzado, trata de personas, o esclavitud por deudas. Esta forma de esclavitud moderna ocurre en casi todos los países del mundo, incluyendo a los países con altos ingresos.

De acuerdo con la revista The Times, la plataforma Haraj, tiene más de un millón de visitantes al día, Haraj se describe a sí misma como la mayor plataforma de compraventa, en ella se pueden adquirir coches, muebles, aparatos electrónicos, animales, y como sugiere una reciente investigación, los seres humanos también están en esta lista[163]. Curiosamente, esta aplicación vende y renta a personas migrantes casi en calidad de objeto. Esta situación los coloca en una situación de desventaja, ya que no gozan de derechos civiles. La persona que da a otra persona (en su mayoría migrantes) en arrendamiento, se llama “Kafala” o “Kafeel”, y esta misma persona es la que se encarga de hacer “trámites legales” y por así decirlo, firma como responsable legal para que cierta persona pueda trabajar en su país, Arabia Saudita[164]. Este sistema de “compraventa” de seres humanos es sin duda alguna, una forma de trata de personas, y es que a pesar de que funciona legalmente en el país, algunos sauditas retienen el pasaporte de sus

[161] DW Español. 2020. Viaje al lado oculto de Internet. [microdocumental] Consultado el 7 de marzo de 2023. Disponible en: https://www.youtube.com/watch?v=bZySuxR8bGM
[162] ONU. 50 millones de personas en el mundo en situación de esclavitud moderna. Consultado el 7 de marzo de 2023. Disponible en: https://mexico.un.org/es/198861-50-millones-de-personas-en-el-mundo-en-situaci%C3%B3n-de-esclavitud-moderna#:~:text=GINEBRA%20%E2%80%93%20Cincuenta%20millones%20de%20personas,estaban%20atrapadas%20en%20matrimonios%20forzados.
[163] Cit. Por DW español. 2023. Cómo se abusa de las aplicaciones para la esclavitud moderna. Consultado el 7 de marzo de 2023. Disponible en: https://www.youtube.com/watch?v=l9RgxmhU1yc
[164] Cfr. por DW español. 2023. Cómo se abusa de las aplicaciones para la esclavitud moderna. Consultado el 7 de marzo de 2023. Disponible en: https://www.youtube.com/watch?v=l9RgxmhU1yc

trabajadores, otros les aplican castigos físicos, y esperan que trabajen sin pausa por menos de seis euros al día[165].

Este ejemplo y los diversos tipos de delitos que se estudiaron en el presente apartado son muy alarmantes, por ello, las tres esferas de cualquier gobierno deben adecuar sus leyes y capacitar a la gente para enfrentarse a los constantes cambios y amenazas de los delincuentes en la internet. En espacial porque como se estudió, cada vez aumenta el número de delitos que ocurren en el internet. Y es que hoy en día los seres humanos trasladan casi todas sus actividades al plano del ciberespacio. Se analizó que, desde la pandemia de 2020, al menos en México más de la mitad de su población comenzó a realizar casi todas sus actividades en línea. Pero cuando las personas desconocen los riesgos que hay en la internet, su navegación en ella puede ser peligrosa. Por ello, es imperante que las organizaciones públicas y privadas, así como sociedad en general, comience a tener una cultura de prevención y autocuidado para prevenir cualquier tipo de ataque en la red, así como aquellas formas de navegar en la internet cuidando sus datos personales y las de otros. Y eso, se analiza mejor en el siguiente apartado.

2.5 Ciberseguridad y datos personales

Hoy en día la tecnología se volvió indispensable para el funcionamiento de nuestras sociedades, y con ello, los retos que se presentan en el día a día para su adecuado funcionamiento son cada vez más complicados y novedosos, al punto de que se necesita de un mejor entendimiento de la situación para una solución eficaz ante cualquier problema. Cuando se presentan dificultades que implican el uso de la tecnología, el escenario es preocupante. En México, por ejemplo, no existe regulación específica que marque la manera de resolver problemas que implican el uso de la tecnología. Además, tampoco existe un marco jurídico de referencia para asuntos de este tipo.

En el presente apartado, se exponen algunos ejemplos en los cuales se vislumbra la necesidad de una adecuada preparación técnica, legal y de recursos humanos para

[165] DW español. 2023. Cómo se abusa de las aplicaciones para la esclavitud moderna. Consultado el 7 de marzo de 2023. Disponible en: https://www.youtube.com/watch?v=l9RgxmhU1yc

hacer frente a cualquier situación que implique proteger los derechos humanos de las personas en la era digital.

a) Para entender el papel del ciberespacio y la ciberseguridad

Para entender mejor el presente capítulo, es necesario conocer los conceptos claves del tema. Y para entender mejor cómo funciona la ciberseguridad, es necesario primero el estudio del ciberespacio. De acuerdo con este orden de ideas, el ciberespacio fue un término que fue introducido primero en el mundo de la ciencia ficción en 1984, por William Gibson, autor de la novela *Neuromante*. De acuerdo con Gibson, "el ciberespacio es una red de almacenamiento de datos digitales con conectividad para acceso e interacción a través de una conexión de computadora"[166].

Trasladado este concepto en el mundo real, el ciberespacio es definido por Romero Galicia como un "dominio creado por el hombre, global, dinámico y en constante cambio, que se encuentra dentro del entorno de información. Consiste en redes interdependientes de infraestructuras de tecnologías de información, incluyendo el internet, redes de telecomunicaciones, sistemas industriales de control y cualquier otro tipo de sistema tecnológico que contenga procesadores y controladores embebidos capaces de ser accedidos de forma remota"[167].

> *"Es importante señalar que el ciberespacio constituye un campo de desarrollo, en el cual se transfiere información económica, social y gubernamental, que debe ser cuidada y es la base de muchos servicios actuales de la sociedad, por lo que es necesario crear políticas que aseguren que este campo esté disponible para que los servicios se establezcan normalidad y fuera de riesgos o acciones contrarias que puedan perjudicar a personas, empresas o gobiernos. Es por ello que se*

[166] Cit. por Romero Galicia, Jaime. Conceptualización de una estrategia de ciberseguridad nacional en México. Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM, vol. XXVIII, núm. 2, 2018. Consultado el 27 de febrero de 2023. Disponible en: https://www.redalyc.org/articulo.oa?id=65458498003
[167] Romero Galicia, Jaime. Conceptualización de una estrategia de ciberseguridad nacional en México. Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM, vol. XXVIII, núm. 2, 2018. Consultado el 27 de febrero de 2023. Disponible en: https://www.redalyc.org/articulo.oa?id=65458498003

han creado políticas y medidas de seguridad del ciberespacio para proteger este campo"[168]*.*

Además, el ciberespacio destaca debido a que es menos costoso para empresas, gobiernos, organizaciones e incluso personas almacenar y tratar su información en la nube, por eso, es mucho más frecuente que las personas hagan mayor uso de las tecnologías de la información. Esta práctica permite ser más eficientes y rápidas a las personas en sus actividades. Se puede decir que el contexto del ciberespacio tiene mayor alcance al considerarse el internet, la nube y las TIC's herramientas globales.

El ciberespacio hoy por hoy es muy importante y su protección muy necesaria, porque ahí tienen lugar muchos procesos productivos y se establece la comunicación de las sociedades, que ha sido considerada militarmente por la mayoría de los países como el quinto dominio de la guerra, aunado a los dominios de tierra, mar, aire y espacio exterior[169].

Una vez comprendido el concepto de ciberespacio, toca turno analizar el papel que juega la ciberseguridad en él. Por lo que se refiere a ciberseguridad, Singer y Friedman argumentan que "la ciberseguridad se entiende como el intento para salvaguardar la integridad y continuidad de los sistemas digitales e informáticos a fin de garantizar los principios de confidencialidad de la información, la integridad en el intercambio seguro de datos, así como la operatividad y disponibilidad de la arquitectura técnica dentro de la infraestructura de las tecnologías de la información y comunicación"[170]. A pesar de que se hace mención sobre mantener seguros los sistemas y tecnologías de la información, la definición no es del todo completa, puesto que no se menciona sobre la protección hacia las infraestructuras críticas de información, las cuales, mantienen una relación estrecha con las tecnologías usadas para procesar, almacenar y tratar datos.

[168] Cit. Por Romero Galicia, Jaime. Conceptualización de una estrategia de ciberseguridad nacional en México. Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM, vol. XXVIII, núm. 2, 2018. Consultado el 27 de febrero de 2023. Disponible en: https://www.redalyc.org/articulo.oa?id=65458498003
[169] *Ibidem.*
[170] Cit. por Patiño Orozco, Germán Alejandro. (2021). Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos. Oasis, n-um. 34, 2021, julio-diciembre, pp. 107-126. Consultado el 28 de febrero de 2023. Disponible en: https://www.redalyc.org/journal/531/53169476007/53169476007.pdf

Por su parte, la ITU (International Telecommunication Union) menciona que “el objetivo de la ciberseguridad es garantizar la seguridad del entorno digital, tanto activos como a usuarios, gracias a la aplicación de estrategias y al empleo de herramientas tecnológicas para la prevención, mitigación, y control de los posibles riesgos cibernéticos que amenacen a una organización”[171]. Es importante destacar que la ITU realizó una evaluación sobre diversos aspectos del estado de la ciberseguridad en 194 países alrededor del mundo durante 2020, en la cual, México ocupa la posición 52. Detecta como puntos de mejora las organizaciones y las estrategias que atienden los temas asociados a la ciberseguridad en la nación, las leyes, y los procesos judiciales en relación con el cibercrimen y el desarrollo de competencias en términos de ciberseguridad[172].

La definición que en este trabajo de investigación se considera más completa es la que ofrece el Departamento de Defensa de Estados Unidos, que define a la ciberseguridad como “la prevención de daños para la protección y restauración de computadoras, sistemas electrónicos de comunicación, servicios de comunicación electrónica, comunicaciones inalámbricas y comunicación electrónica, incluyendo información contenida en ellos, para asegurar su disponibilidad, integridad, autenticidad, confidencialidad y no repudio”[173].

Además, la ciberseguridad tiene que ver con un concepto más amplio, que es la seguridad de la información, definida como la protección de la integridad, confidencialidad y disponibilidad de los datos, independientemente de donde se procesen, transmitan o almacenen[174].

Por lo tanto, el ciberespacio y ciberseguridad son conceptos que, de acuerdo con las prácticas de los últimos años, tienen un papel muy importante para las estrategias de

[171] Cit. por Matilde-Espino, Yesenia y Valencia-Pérez, Luis-Rodrigo. 2022. Análisis bibliométrico de la producción científica sobre México en temas de ciberseguridad (2015-2020). CIENCIA ergo-sum, Revista Científica Multidisciplinaria de Prospectiva. Consultado el 22 de febrero de 2023. Disponible en: https://www.redalyc.org/journal/104/10472165009/10472165009.pdf
[172] *Ibidem.*
[173] Cit. por Romero Galicia, Jaime. (2018). Conceptualización de una estrategia de ciberseguridad para la seguridad nacional de México. Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM, vol. XXXVIII, núm. 2. Consultado el 28 de febrero de 2023. Disponible en: https://www.redalyc.org/articulo.oa?id=65458498003
[174] *Ibidem*.

seguridad en cada país. Y México, no es la excepción. Las mismas cualidades y características del ciberespacio hacen que esta materia sea una excelente opción para incentivar el desarrollo y la eficiencia en los procesos para brindar bienes y servicios, pero también implica un gran reto el tratar y proteger de una adecuada manera la información que contenga el ciberespacio, porque como se mencionó anteriormente, el ciberespacio se conforma por cualquier tipo de redes interdependientes de infraestructuras de tecnologías de información que son usados por cualquier industria, sea pública o privada. Desde esta visión, estas infraestructuras de tecnologías de la información se convierten en unos de los principales objetivos a atacar por parte de gobiernos extranjeros, ciberdelincuentes, o cualquier particular que tenga la intención de afectar a una, decenas, miles o millones de personas.

b) ¿Qué son las infraestructuras críticas y por qué existen ataques hacia ellas?

Hoy en día casi todas las sociedades, pero en especial las sociedades más desarrollas y semidesarrolladas poseen infraestructuras físicas o digitales que son necesarias para brindar cualquier tipo de servicio o bien a la sociedad en general.

Una infraestructura crítica de la información (ICI) está íntimamente relacionada con las infraestructuras críticas y la protección de infraestructuras críticas de una nación. Las infraestructuras críticas de información se definen como “aquellas infraestructuras de información y comunicaciones interconectadas que son esenciales para mantener funciones sociales vitales (bienestar social, económico, de seguridad o de salud de la gente)”[175]. Por consiguiente, la protección a las infraestructuras críticas de la información es “todas las actividades dirigidas a asegurar la funcionalidad, continuidad e integridad de las ICI para disuadir, mitigar y neutralizar las amenazas, riesgos o vulnerabilidades, o minimizar el impacto de un accidente”[176].

Originalmente, las infraestructuras críticas fueron creadas para proveer de servicios y bienes a la población de un lugar determinado. Con el paso del tiempo, estas

[175] Global Forum on Cyber Expertise. The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection. Consultado el 28 de febrero de 2023. Disponible en: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf
[176] *Ibidem*.

infraestructuras críticas se volvieron vitales para el funcionamiento de las sociedades. En los últimos años, muchas de estas infraestructuras se conectaron a internet y aumentaron su uso de las tecnologías de la información. En la actualidad, muchas de estas infraestructuras dependen casi en su totalidad de la tecnología digital y de la internet.

Los ciberataques a las infraestructuras críticas quizá son mucho menos comunes, pero sí más fatídico. Por ejemplo, de acuerdo con una investigación realizada por DW español, cita que los aerogeneradores de Alemania pueden estar conectados a satélites estadounidenses para funcionar bien, y una disrupción a la comunicación de estos satélites y los aerogeneradores puede dejar sin energía la infraestructura crítica de toda una sociedad[177].

En un panorama actual, los hackers ya han atacado las infraestructuras críticas de diversos países. En 2019 los atacantes irrumpieron en la red de la mayor central nuclear de la India. En 2021 un ataque a un proveedor de gaseoductos provocó compras de pánico y escases de gas en Estados Unidos, y en 2022 los hackers paralizaron los sistemas informáticos del gobierno de Costa Rica[178]. Pero los hackers no sólo buscan un fin monetario al tomar como “rehenes” a estas infraestructuras críticas, algunos gobiernos, servicios secretos, empresas o personas en general, pueden ocupar métodos de hackeo similares para infundir miedo y pánico entre la población y así obtener alguna ventaja en particular.

En 2017, México y otros 149 países sufrieron un ciberataque a nivel mundial, a través del programa “*WannaCry*”, el cual operaba mediante extorsiones, ya que tenía la función de “secuestrar” información para luego “pedir pagos por su rescate”; este es el *modus operandi* típico de un ransomware. Se calcula que el número de víctimas de este malware, hasta el 2018, fue de al menos 200,000 a nivel mundial; mientras que, en México, se estima que el 44% de las organizaciones fueron víctimas del secuestro de su

[177] Brockmann, Anija y Kroll, Katharina. (2022) Infraestructura digital crítica: ¿por qué hay cada vez más ciberataques? [vídeo]. DW Español. Consultado el 28 de febrero de 2023. Disponible en: https://www.youtube.com/watch?v=bUI9oeulGAU
[178] *Ibidem.*

información[179]. En 2021, el malware bancario “Janeleiro” fue creado originalmente para atacar corporativos de bancos en Brasil, del cual fue creada una variante para atacar usuarios en México, y poder robar su información bancaria y personal. Este virus es distribuido a través de correos electrónicos, que contienen enlaces que redireccionan a los usuarios ventanas emergentes con formularios de banco apócrifos; de esta forma logran acceder y robar la información bancaria[180].

Teniendo en cuenta lo anterior, importa preguntarse qué estamos haciendo para evitar que esto suceda. Para evitar los ciberataques y mejorar la ciberseguridad, es importante, primero que nada, actualizar con regularidad los sistemas informáticos empleados para nuestras actividades, sobre todo aquellas que se enfocan en atender las infraestructuras críticas; también es crear una excelente cultura de autocuidado y prevención de riesgos en el ciberespacio, para que cuando surja una situación de esta índole, reaccionar rápidamente para solucionar cualquier hackeo o ciberdelito.

A diferencia de los hackers maliciosos con el objetivo de dañar a alguien o algo, también existen aquellos que se dedican a detectar fallos de seguridad en sistemas informáticos o que hackean sistemas con información relevante y de interés público. En este sentido, es importante resaltar que los llamados hacker éticos o *hacktivistas*, son de gran ayuda para encontrar y entender los puntos débiles de los sistemas informáticos de cualquier organización o persona. Además, en algunos casos, dejan mostrar a la sociedad cómo algunas organizaciones o incluso Estados, recaban, organizan, clasifican y tratan cierta información o situación de un lugar específico. Por ejemplo, los *hacktivistas* del grupo “Guacamaya” en septiembre de 2022 hackearon los servidores de la SEDENA, en los cuales se deja en claro que algunos gobiernos recaban información y datos personales que involucra directamente a personas o activistas. De acuerdo con una nota elaborada por la BBC, la SEDENA habría adquirido el software de espionaje “*Pegasus*” con el cual se espiaba a civiles[181], grupos activistas, feministas, entre otros. Esta serie de

[179] Equipo ORCA. 2019. 3 casos reales de delitos informáticos en México. Consultado el 7 de marzo de 2023. Disponible en: https://blog.orcagrc.com/casos-de-delitos-informaticos-en-mexico
[180] *Ibidem*.
[181] BBC News Mundo. 2022. Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México. Consultado el 6 de marzo de 2023. Disponible en: https://www.bbc.com/mundo/noticias-america-latina-63167331

declaraciones que salieron a la luz, indican que el Estado y el ejército ve a los defensores de derechos humanos como potenciales amenazas. Los documentos filtrados exponen diversos temas que tuvieron mucho interés en la población. En cuanto a los datos personales y el derecho a la privacidad, se mostró que algunos de los documentos y servidores de la SEDENA recaba el nombre e imagen de las principales organizadoras de los movimientos y de las marchas feministas y no feministas, así como lugares en los cuales se realizan las reuniones, los encuentros, los lugares en donde se realizan daños materiales, entre otros. Una de las defensoras por los derechos de las mujeres en México menciona que el hecho de que "el ejército tenga cada vez más poder en el país preocupa a las feministas porque, dicen, las pone en la mira de futuros ataques"[182]. Una más argumenta que "conocer que el ejército está espiando a las feministas inhibe la protesta, te da miedo lo que pueda pasar y la gente deja de salir a las calles. Eso es el militarismo. La sola idea hace que la gente se calle genera una conducta social distinta, mucho menos libre"[183].

Todos los ejemplos que en este capítulo se estudiaron, muestran cómo la internet, la IA, y en general el ciberespacio influye de distintas maneras en nuestra vida. Por ello, resaltar la importancia que tiene el respeto y efectiva protección de los datos personales. Todos los casos analizados, no limita el poder que tiene el Estado y las empresas hacia los ciudadanos dentro de la red. Siendo así que, en la actualidad, algunos gobiernos que respetan menos los derechos humanos comienzan a analizar los comportamientos de las personas para, en lo que a ellos les convenga, modifiquen el comportamiento de la población o les infundan miedo al castigar con severidad ciertos actos.

2.6 Recomendaciones para implementar ciberseguridad y evitar ser víctimas de ciberdelitos

Durante todo este apartado se mostró que la aparición de las nuevas formas criminales, como la ciberdelincuencia y el ciberterrorismo, hicieron que organizaciones como la ONU y la Unión Europea (EU) -principalmente- hayan tenido que adaptar su ordenamiento

[182] Cir. Por Barragán, Almudena. 2022. El ejército mexicano ve a las feministas como enemigas del Estado. Disponible el 6 de marzo de 2023. Disponible en: https://elpais.com/mexico/2022-10-23/el-ejercito-mexicano-ve-a-las-feministas-como-enemigas-del-estado.html
[183] *Ibidem*.

jurídico para garantizar la seguridad de los ciudadanos. En México, la legislación en materia de ciberseguridad no existe como tal. Sólo algunas leyes y reglamentos mencionan el tema de la ciberseguridad, como la Constitución mexicana, la Ley Federal de Protección de Datos Personales en Posesión de Particulares, la Ley General de Títulos y Operaciones de Crédito, el Código Penal, y la Estrategia Nacional de Ciberseguridad de 2017; sin embargo, es necesario una ley específica para la subsecuente creación de programas nacionales, instituciones y delitos en específico. Una vez que exista esta ley, será necesaria la adecuación de esta ley con otras ya existentes. Además, estas modificaciones y adaptaciones legislativas tienen que ir acompañadas de otras líneas de acción concretas, que implican crear y organizar nuevas estructuras que bajo la dirección ejecutiva de los gobiernos podrían ir poniéndose en marcha dentro de un plan estratégico integral[184]. Por eso es necesaria una excelente y actualizada cultura de la ciberseguridad, ya que su conocimiento brinda las bases para entender mejor cómo proteger nuestros datos y nuestra vida en la internet. Un dato interesante dado por la Asociación de Internet en su Estudio sobre ciberseguridad en empresas, personas usuarias de internet y padres de familia en México muestra que a pesar de que la mayor proporción de usuarios (90.6%) menciona que le preocupa la ciberseguridad, sólo el 50% de los encuestados menciona que sus equipos están protegidos ante las amenazas que presenta el uso de internet, demostrando que en México existe una baja cultura para la prevención de delitos digitales[185].Por ello es necesario que cualquier institución ofrezca capacitaciones constantes para mantener seguros nuestros datos. En este sentido, en este trabajo de investigación se proporciona de manera explicativa, más no limitativa, algunas recomendaciones dadas por Colón Ferruzola y Cuenca Espinosa para evitar ser víctima de los delitos:

[184] Pons Gamón, Vicente. 2017. Internet, la nueva era del ciberdelito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad, núm. 20. ISSN: 1390-3691. Consultado el 8 de marzo de 2023. Disponible en: https://www.redalyc.org/articulo.oa?id=552656641007

[185] Asociación de Internet. 2022. Estudio sobre ciberseguridad en empresas, personas usuarias de internet y padres de familia en México. Consultado el 7 de marzo de 2023. Disponible en: https://irp.cdn-website.com/81280eda/files/uploaded/Encuesta%20Ciberseguridad%202022%20pu%CC%81blica%202 0230119.pdf

- “Tener instalado en sus equipos informáticos un antivirus y antispyware con licencia y actualizados.
- Tener instalado en nuestros equipos informáticos las actualizaciones recientes de seguridad.
- Para acceder a cuentas bancarias y de correo electrónico, utilizar el teclado virtual para mayor seguridad.
- No acceder a páginas de contenido pornográfico, ya que en su mayoría contienen virus.
- Evitar descargar programas gratuitos porque la mayoría son infecciosos.
- Evitar instalar programas crackeados, piratas o con parches.
- Realizar un análisis con el antivirus actualizado de todo dispositivo de almacenamiento de información que conectemos a nuestro equipo.
- Revisar con cautela los correos que tengamos en la bandeja de entrada, estos pueden ser spam, contener código malicioso que nos puede redireccionar a un sitio falso donde al ingresar nuestros datos podemos ser víctimas de robo de información.
- Tenga cuidado con los negocios, promociones, inversiones y regalos por internet, la mayoría de las veces contienen virus o son estafas.
- No proporcionar nunca información personal sobre ti a través de internet a personas desconocidas, evitar tomar fotos de tarjetas de crédito, cédula, DNI, pasaporte o visa y subirlo a redes sociales como Instagram, Facebook o Twitter.
- No responder a mensajes de anuncios o cadenas en los que se incluyan mensajes agresivos, obscenos o amenazantes. No pactes citas con personas desconocidas. Instale la computadora en un área de fácil acceso a todos los miembros de la casa, para poder vigilar su uso por los menores. Si sus hijos son pequeños no les permita entrar en chats y redes sociales sin tener a un adulto presente. No permita que sus hijos pacten citas por Internet.
- No envíe información bancaria o crediticia a través de correos electrónicos, los bancos nunca solicitan este tipo de información por medio de un correo electrónico o mensajes de texto.

- Cuando cree su clave, use siempre palabras combinadas con números, letras y símbolos diferentes, no utilices datos personales, nombre de hijos o familiares.
- Muchos hackers utilizan noticias curiosas o impactantes para lanzar infecciones, troyanos, malware a través de enlaces a páginas web, por lo que no es recomendable abrir los documentos.
- No descargar software del cual no se tenga plena confianza de que son sitios seguros ni tampoco abrir archivos o postales de desconocidos enviados a los correos, las direcciones seguras son una forma de verificar que el sitio a donde se ingrese es verídico, la forma de reconocerlos es que la página empiece con https:/"[186].

Una vez analizado de manera general el gran panorama en el cual están nuestros datos personales, desde el ámbito comercial, político, tecnológico, y de seguridad, es importante que en esta investigación se analicen las distintas garantías legales que permiten la defensa y protección de los datos personales. Para ello, se destinan el capítulo III y IV para conocer más sobre ellas.

[186] Colón Ferruzola Gómez, E., & Cuenca Espinosa, H. A. (2014). Cómo responder a un Delito Informático. Revista Ciencia Unemi, 7(11),43-50. [fecha de Consulta 8 de Marzo de 2023]. ISSN: 2528-7737. Recuperado de: https://www.redalyc.org/articulo.oa?id=582663858004

CAPÍTULO III. EL *HABEAS DATA* COMO MECANISMO DE PROTECCIÓN DE LOS DATOS PERSONALES.

El presente capítulo pretende dar un primer acercamiento para conocer el mecanismo legal por excelencia para el ejercicio del respeto a los datos personales. Es, además, la introducción a la historia del Habeas Data, el mecanismo que permite a las personas conocer quién y cómo tratan sus datos personales, y también para evitar que esos mismos datos se sigan usando.

3.1 Concepto de Hábeas Data.

Partiendo desde un análisis etimológico, el habeas data tiene como antecedente el "habeas corpus". *Habeas* significa tener en posesión, y "data" proviene del inglés que significa datos; así entonces, *habeas data* significa "tener los registros o tener los datos".

De acuerdo con Palazzi, el "habeas data puede ser concebido como una acción judicial para acceder a registros o bancos de datos, conocer los datos almacenados y en caso de existir falsedad o discriminación corregir dicha información o pedir su confidencialidad"[187].

Por su parte, Hernández define al Habeas Data como "una construcción conceptual para englobar todos aquellos elementos sustantivos y procedimentales creados para la protección de la persona frente al tratamiento de sus datos personales"[188]. Menciona además que el habeas data "se ha convertido en una mera garantía procedimental para proteger al derecho que tiene la persona al acceso y conocimiento de sus datos personales en registros públicos y privados"[189]. De acuerdo con este autor, el habeas

[187] Cit. por Oberto de Grude, Lucía; Govea de Guerrero, María. 2008. Algunas consideraciones sobre el habeas data en Venezuela. Télématique: Revista Electrónica de Estudios Telemáticos, ISSN-e: 1856-4194. Consultado el 15 de marzo de 2023. Disponible en:
https://dialnet.unirioja.es/servlet/articulo?codigo=2954091

[188] Hernández, Juan Carlos. 2012. La protección de datos personales en Internet y el habeas data. Corte IDH. ISSN: 1317-9306. Consultado el 15 de marzo de 2023. Disponible en:
https://www.corteidh.or.cr/tablas/r32012.pdf
En el mismo sentido está en Torres, R. (2022). Régimen jurídico de la transparencia y acceso a la información pública gubernamental, datos personales y big data. [Tesis de maestría, Universidad Nacional Autónoma de México]. Repositorio institucional de la Universidad Nacional Autónoma de México.
http://132.248.9.195/ptd2022/diciembre/0833896/Index.html

[189] *Ibidem.*

data es meramente un mecanismo legal para conocer quién y cómo trata nuestros datos personales, no es tanto un mecanismo que dé pauta a la prevención de un tratamiento ilegal.

Desde sus orígenes, el habeas data sirvió para lograr acceder a cualquier banco de información, sea pública o privada. De acuerdo con la historia del habeas data, los legisladores crearon esta figura jurídica con el objetivo de garantizar que cualquier persona, sea física o jurídica colectiva, accediera a su propia información. Pero eso no implicaba que se pudiera solicitar la rectificación, la oposición a algún tratamiento, o pedir la cancelación total o parcial de dichos datos. Tampoco garantizaba una protección jurídica y reparación de daños a la persona o su familia, en el supuesto de que existiese información falsa sobre ella o hubiese un mal tratamiento de sus datos. Hoy en día, Oberto y Govea argumentan que "este instrumento jurídico permite gestionar el dato en cuestión de una forma rápida y urgente, para subsanar la falsedad que pueda implicar. Así mismo sirve para acceder a la información relativa al afectado de manera directa ya que se trata de una herramienta jurídica destinada a la prevención y defensa de las personas contra toda posible lesión y en resguardo de la buena fe de la información"[190].

En resumen, el habeas data es una figura jurídica – que existe en algunos países- para ejercer el derecho de autodeterminación informativa; así como los derechos ARCO (acceso, rectificación, cancelación y oposición) de nuestra información contenida en bancos de datos pública o privada. Y como se estudiará a lo largo del capítulo, algunos tipos de habeas data permiten ser más específicos en el cuidado y tratamiento seguro de los datos personales.

[190] Oberto de Grude, Lucía; Govea de Guerrero, María. 2008. Algunas consideraciones sobre el habeas data en Venezuela. Télématique: Revista Electrónica de Estudios Telemáticos, ISSN-e: 1856-4194. Consultado el 15 de marzo de 2023. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=2954091

3.2 Evolución histórica del *Hábeas Data.*

A pesar de que la historia del habeas data es reciente, la base de la inspiración para la creación de este instrumento jurídico nace con la Declaración Universal de los Derechos Humanos y diversos tratados internacionales.

Cabe destacar que los países de la Unión Europea le dieron prevalencia al tema de la privacidad, inclusive más allá de los intereses comerciales de las empresas, con el propósito de salvaguardar y proteger los derechos y libertades de las personas físicas, en particular el derecho a la intimidad y la libre circulación de datos personales, derechos consagrados en las Constituciones y leyes de los Estados miembros y el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

a) Evolución en Europa.

En Alemania, Brigard y Urrutia mencionan que el Derecho de habeas data se remota a la primera ley de protección de datos llamada *Bundesdatenschutzgesetz*[191] que se emitió el 7 de octubre de 1970[192]. Por su parte, Oberto y Govea mencionan que "en el año de 1973 cuando se sancionó la Primera Ley Nacional de Protección de datos del mundo y fue en Suecia, luego en 1974 en Estados Unidos, las agencias estatales se vieron obligadas a seguir ciertas directrices en la utilización de información personal en donde se debía exigir la notificación del informado por la acumulación de sus datos. Hoy en día el habeas data es un derecho reconocido en varios países como Austria, Francia, Suecia, Chile, Alemania, Colombia, Brasil, entre otros".[193]

Por su parte la Comisión Interamericana de Derechos Humanos, en su Informe de la Relatoría para la Libertad de Expresión de 1999, en relación con el habeas data

[191] "*Ley Federal de Protección de Datos"*, traducida al español.
[192] Cit. por Parraguez Kobek, Luisa y Caldera, Erick. 2016. Cyber Security and *Habeas Data*: The Latin Amreican Response to Information Security and Data Protection. Oasis, no. 24, pp. 109-128. Consultado el 15 de marzo de 2023. Disponible en: https://www.redalyc.org/journal/531/53163716007/html/index.html#B2
[193] Oberto de Grude, Lucía; Govea de Guerrero, María. 2008. Algunas consideraciones sobre el habeas data en Venezuela. Télématique: Revista Electrónica de Estudios Telemáticos, ISSN-e: 1856-4194. Consultado el 15 de marzo de 2023. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=2954091

argumenta que “mediante este procedimiento se garantiza a toda persona a acceder a información sobre sí misma o sus bienes contenida en bases de datos o registros públicos o privados y, en el supuesto de que fuera necesario, actualizarla o rectificarla”[194]. Este procedimiento de acceso a la información de nuestros datos personales adquirió gran relevancia con la llegada de las diversas plataformas online, redes digitales, de las tecnologías de la información y del internet.

En la década de 1980, Chirino estipula que el tribunal constitucional alemán definió el habeas data como el “derecho a saber qué tipo de datos se almacenan en bases de datos manuales y automáticas sobre el individuo”[195]. Luego en 1981 se estableció el 108 Convenio sobre Protección de Datos decretado por el Consejo de Europa que en términos generales establece el derecho que tiene cualquier persona dentro de la Unión Europea para saber quién, cómo y para qué fines recaba y trata sus datos personales. Hoy en día, México ratificó ante el senado dicho Convenio. Eventualmente, más estados dentro de la Unión Europea agregaron leyes de protección de datos, como Gran Bretaña en 1984[196].

En 1995 fue aprobada la Directiva 95/46 del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos (mejor conocida como la Directiva sobre privacidad y protección de datos personales), que entró en vigor el 25 de octubre de 1998 con el objeto de proporcionar un marco general de referencia para los países miembros. Esta directiva establece reglas muy estrictas para la protección de los derechos y garantías de libertad de los ciudadanos europeos y en particular la protección del derecho a la privacidad con relación a la obtención y procesamiento de los datos

[194] Informe anual del relator especial para la libertad de expresión. 1999. OEA. Consultado el 15 de marzo de 2023. Disponible en: https://www.oas.org/es/cidh/expresion/docs/informes/anuales/Informe%20Anual%201999.pdf

[195] Cit. Por Parraguez Kobek, Luisa y Caldera, Erick. 2016. Cyber Security and *Habeas Data*: The Latin Amreican Response to Information Security and Data Protection. Oasis, no. 24, pp. 109-128. Consultado el 15 de marzo de 2023. Disponible en: https://www.redalyc.org/journal/531/53163716007/html/index.html#B2

[196] Parraguez Kobek, Luisa y Caldera, Erick. 2016. Cyber Security and *Habeas Data*: The Latin Amreican Response to Information Security and Data Protection. Oasis, no. 24, pp. 109-128. Consultado el 15 de marzo de 2023. Disponible en: https://www.redalyc.org/journal/531/53163716007/html/index.html#B2

personales[197]. Una de las principales críticas que se le hace a esta directiva es el artículo 25, el cual contiene fuertes restricciones en cuanto al flujo transfronterizo de datos, lo cual limita el alcance que podría tener en cuanto al comercio electrónico internacional con otros países como EUA o China[198].

b) EUA.

Estados Unidos de América (EUA) mantiene hasta el día de hoy una política de autorregulación para que los Estados y las empresas adecuen las leyes en materia de privacidad y protección de datos de acuerdo con el surgimiento de las nuevas tecnologías. Esto se debe en gran medida a que este el principal país que fomenta el comercio electrónico, además de que en este país es la cuna de nacimiento de diversas empresas tecnológicas a nivel mundial. Esta práctica permite que EUA sea uno de los países líderes en comercio electrónico internacional y de tecnología.

Esta práctica de autorregulación permite a las corporaciones establecer sus propios estándares de protección de datos personales, de acuerdo con los ya establecidos en algunas leyes. Además, la autorregulación permitía que las empresas adecuaran sus prácticas de la mano con sus innovaciones -principalmente tecnológicas-, y esto hacía ver a la sociedad como protegida por estas corporaciones.

La rápida innovación de las tecnologías de la información se debe en parte a la demanda del mercado de tales tecnologías y servicios que se usan para su mejor funcionamiento. Este es el punto que tanto Estados Unidos como Europa tienen en cuenta a la hora de establecer normativas; sin embargo, EE. UU. tiende a legislar en conjunto con el mercado global[199]. Por el contrario, Higgott argumenta que Europa ha “desarrollado marcos

[197] Hernández, Juan Carlos. 2012. La protección de datos personales en Internet y el habeas data. Corte IDH. ISSN: 1317-9306. Consultado el 15 de marzo de 2023. Disponible en: https://www.corteidh.or.cr/tablas/r32012.pdf

[198] Cfr. En Hernández, Juan Carlos. 2012. La protección de datos personales en Internet y el habeas data. Corte IDH. ISSN: 1317-9306. Consultado el 15 de marzo de 2023. Disponible en: https://www.corteidh.or.cr/tablas/r32012.pdf

[199] Parraguez Kobek, Luisa y Caldera, Erick. 2016. Cyber Security and *Habeas Data*: The Latin Amreican Response to Information Security and Data Protection. Oasis, no. 24, pp. 109-128. Consultado el 15 de marzo de 2023. Disponible en: https://www.redalyc.org/journal/531/53163716007/html/index.html#B2

regulatorios sofisticados a través de su arquitectura institucional y la cristalización efectiva del comercio internacional, la inversión y otras políticas comunes”[200].

Hasta el día de hoy, y principalmente Estados Unidos sigue una práctica de autorregulación, sin embargo, no es del todo la más eficaz. Ya que si bien las empresas designan lineamientos de protección a los datos personales es difícil saber con precesión que tan bien se protegen los derechos humanos. En resumen, no existe alguna garantía pública por parte de algún organismo público que verifique y valide las prácticas de autorregulación por las empresas. Al respecto Mendel argumenta que “en muchas ocasiones, los esquemas de autorregulación han servido para simular el cumplimiento y encubrir los verdaderos intereses de las empresas”[201].

Por todo lo anterior, el esquema de autorregulación debe de coexistir con un esquema de regulación vinculante que permita a el Estado involucrarse en el respeto de los derechos humanos y la efectiva protección de datos personales. El esquema de autorregulación no es del todo malo, pero se debe de permitir la intervención equilibrada del Estado, asumiendo su papel de emitir normas que briden los principios básicos y actualizados para el respeto de los derechos humanos en la era digital. Así mismo, el Estado no debe de renunciar a su papel como juzgador a través de los tribunales para asuntos que impliquen una mala recolección, tratamiento y transferencia de los datos personales.

c) Evolución en América Latina

Los países en América Latina encontraron principalmente inspiración en las leyes de la Unión Europea para implementar el Habeas Data en cada uno de sus respectivos países. Esto se debe principalmente a que en América Latina el desarrollo tecnológico fue menor que en Europa, Asia o en América del Norte. Ahora, con la rápida expansión de las tecnologías de la información y del internet en la región, se hizo necesario que los

[200] Cit. por Parraguez Kobek, Luisa y Caldera, Erick. 2016. Cyber Security and *Habeas Data*: The Latin Amreican Response to Information Security and Data Protection. Oasis, no. 24, pp. 109-128. Consultado el 15 de marzo de 2023. Disponible en: https://www.redalyc.org/journal/531/53163716007/html/index.html#B2

[201] Cit. Por Quijano, Carmen. 2022. Derecho a la privacidad en internet. Tirant Lo Blanch. Ciudad de México. Pág. 221.

diversos países que la conforman adecuaran sus leyes para proteger los intereses y derechos de las personas ante los diversos peligros que tiene la internet.

Originalmente la idea del Habeas Data era acceder a cualquier banco de datos sea público o privado, para conocer quién y cómo tratan los datos personales. Hoy en día, este mecanismo legal sirve para amparar a cualquier persona que acceda al ciberespacio y deposite en él sus datos personales.

El primer país americano en incorporar constitucionalmente disposiciones específicas fue Guatemala, que en su Constitución de 1985, dispuso:

> "Art. 31. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos"[202].

Luego, en la Constitución de Nicaragua de 1987, se estableció:

> "Art. 26. Toda persona tiene derecho: 1. A su vida privada y la de su familia. 2. A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo. 3. Al respeto de su honra y reputación. 4. A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información"[203].

Sin embargo, estas disposiciones constitucionales no garantizaban una eficiente hacia los datos personales, puesto que sólo involucraba el acceso a las bases de datos públicos o privados para saber quién y cómo los datos personales.

Fue con la reforma de 1998 que en la Constitución de Ecuador que se regula de manera más amplia el Habeas Data, redactándose de la siguiente manera:

---

[202] Puccinelli, Oscar Raúl. 2004. Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina. Un intento clasificador con fines didácticos. Vniversitas, núm. 107. Consultado el 16 de marzo de 2023. Disponible en: http://www.redalyc.org/articulo.oa?id=82510714

[203] *Ibidem*.

> “Art. 94. Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional”[204].

Otra de las primeras constituciones en América Latina que comenzaba a precisar el Habeas Data, fue la Constitución de Venezuela de 1999, ya que garantizaba los hoy conocidos derechos ARCO en su artículo 28, que a la letra especificaba:

> “Art. 28. Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley”[205]

Además, esta Constitución comienza a distinguir al Habeas Data colectivo, ya que en su artículo 281, menciona las atribuciones del Defensor del Pueblo, entre las que destacan,

[204] *Ibidem*.
[205] Constitución de la República Bolivariana de Venezuela. 1999. Consultado el 16 de marzo de 2023. Disponible en: https://www.oas.org/dil/esp/constitucion_venezuela.pdf

interponer el habeas data colectivo. De ahí que Puccinelli, argumente que esta "norma contiene cuanto menos, tres aciertos: el primero, el de incluir la versión de *Habeas data* impropio, que había sido incorporado por primera vez en la Constitución peruana; el segundo, el de extender la garantía de confidencialidad de la fuente de la información a otras profesiones distintas del periodismo, y el tercero, que constituye una novedad distintiva, el reconocimiento de la facultad del defensor del pueblo de interponer la acción de *Habeas data*, lo que en definitiva puede considerarse la partida de nacimiento normativa del *Habeas data* colectivo[206].

d) Evolución en México.

La historia del habeas data en México es relativamente nueva. En nuestro país, a nivel nacional y en la mayoría de las entidades federativas, no se cuenta aún con una legislación especial sobre el ejercicio de hábeas data o protección a los datos personales; no obstante, diversas legislaciones secundarias han suplido esa ausencia, que, de un modo u otro, tutelan el ejercicio del hábeas data y protegen el segundo de los mencionados. Del conjunto de leyes aludidas, en primer término, se mencionan las leyes de transparencia y/o de acceso a la información pública, que cada entidad federativa ha emitido con sus distintas denominaciones[207].

En México, el habeas data se menciona de manera intrínseca, más no expresa en su artículo 16 constitucional, que a la letra dice:

> "Art. 16 […] **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

[206] Puccinelli, Oscar Raúl. 2004. Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina. Un intento clasificador con fines didácticos. Vniversitas, núm. 107. Consultado el 16 de marzo de 2023. Disponible en: http://www.redalyc.org/articulo.oa?id=82510714
[207] Consideraciones sobre el habeas data y su regulación en distintos ámbitos. Instituto de Transparencia e Información Pública de Jalisco. Consultado el 22 de marzo de 2023. Disponible en: https://www.itei.org.mx/v3/documentos/estudios/estudio_habeas_data_6abr10.pdf

de orden público, seguridad y salud públicas o para proteger los derechos de terceros”[208].

Se puede decir que este artículo es el antecedente más claro sobre una aproximación al habeas data, pero en definitiva, lo es para la protección de datos personales, junto con el artículo 6 constitucional mexicano, que menciona:

> “Art. 6, inciso A. fracción II: […] **La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes”**[209].

Además, este artículo proporciona las bases legales para que los organismos autónomos especializados e imparciales proporcionen los mecanismos legales para el ejercicio del derecho de protección de datos personales, que a la letra dice:

> “III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá **acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos**.
>
> IV. **Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos** que se sustanciarán ante los organismos autónomos especializados e imparciales que establece esta Constitución”[210].

De ahí en adelante que las leyes secundarias creadas para protección de datos personales, así como las reformas o adiciones a los diversos códigos de los Estados surjan a raíz de estos dos principales artículos, que brindan las bases jurídicas de la protección a los datos personales y del derecho a la privacidad. Al respecto, el análisis de estos artículos y leyes, así como a los mecanismos legales de protección de los datos personales se tratarán en el siguiente capítulo.

---

[208] Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. 2022. Consultado el 16 de marzo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf
[209] Artículo 6 de la Constitución Política de los Estados Unidos Mexicanos. 2022. Consultado el 16 de marzo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf
[210] *Idem*.

3.3 Objetivo del Hábeas Data.

En cualquier tipo de habeas data, se vislumbran diversos objetivos, entre los que se encuentran el derecho que tiene toda persona de acceder a la información que sobre ella conste en requisitos o bancos de datos; que se actualicen los datos atrasados; que se rectifiquen los inexactos; que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros y su supresión en los procesos de obtención de información del requisito de la llamada información sensible entre los que cabe destacar la vida íntima, ideas políticas, religiosas entre otros[211].

3.4 Características del habeas data

Es habeas data se caracteriza principalmente por ser un instrumento legal que permita al titular de los datos personales conocer cómo se recaban sus datos, quién lo hace, a través de qué medios, de qué forma, entre otros. Así de esta manera la persona que recurra a este instrumento jurídico ejerce su derecho de autodeterminación informativa. Primero porque requiere saber de qué manera su información se encuentra en bases de datos públicos o privados. Y segundo, porque elige quién, cómo e incluso hasta qué momento su información se contendrá en dichas bases de datos. En este sentido, Sánchez argumenta al respecto “que entendido como derecho constitucional, protegido natural y jurídicamente por el Estado, el habeas data es una institución que le permite a una persona acceder a todo registro de datos, tanto público como privados, sin importar su finalidad para tener conocimiento de éstos y en caso de existir falsedad o discriminación, contar con un instrumento de carácter procesal que le permita cubrir los fallos que se incurran en la exposición, manejo y procesamiento de la información”[212].

[211] Oberto de Grude, Lucía; Govea de Guerrero, María. 2008. Algunas consideraciones sobre el habeas data en Venezuela. Télématique: Revista Electrónica de Estudios Telemáticos, ISSN-e: 1856-4194. Consultado el 15 de marzo de 2023. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=2954091

[212] *Idem*.

Otra característica del habeas data es que este es un mecanismo que garantiza la tutela del ejercicio de otros derechos, entre los que se encuentran el derecho a la intimidad, al honor, a la privacidad, la imagen, entre otros que se estudiaron en el capítulo I (primero). Asimismo, el habeas data permite a una persona ejercer en todo o en parte sus derechos ARCO, puesto que no siempre se requiere de la rectificación, cancelación u oposición de cierta información. Su funcionamiento varía dependiendo del asunto en concreto.

A modo de propuesta, más no de característica, el habeas data debe de adquirir un rango de derecho humano, o al menos, ser reconocido por varios países bajo los mismos lineamientos. Porque cuando se presenta algún problema que relaciona a dos o más países, la forma de resolver el asunto se complica un poco. Hay algunos autores que proponen usar las normas del derecho internacional privado; algunos otros, hacen referencia a usar la norma del país en donde se encuentre el sujeto que fue víctima de algún delito informático o que sus datos personales hayan sido vulnerados. Algunos otros mencionan que se debe de atender a la jurisdicción del lugar en donde se cometió el delito, pero aún así, esto no es tan conveniente, ya que las legislaciones de algunos países ni siquiera garantizan la protección de algunos derechos humanos.

En resumen, el habeas data es un mecanismo jurisdiccional que hoy en día a cobrado mayor relevancia, y que debería ser protegido por todos los países, ya que en un mundo donde casi todas las personas se conectan al internet y usan distintas tecnologías (incluyendo la inteligencia artificial), los datos personales se vuelven más vulnerables ante cualquier situación de peligro o riesgo.

3.5 Derechos tutelados por el habeas data.

De manera general, el habeas data tiene un doble uso (uno de acceso a conocer cierta información de uno mismo y otro a la protección de esos datos), por lo que diversos derechos están titulados por él, como el derecho a la privacidad, el derecho a la intimidad, al honor, a la imagen, de autodeterminación informativa, y la protección de datos personales.

De acuerdo con Muñoz,

> “el recurso de *habeas data* o el derecho de autodeterminación informativa tiene como objetivo fundamental la protección de la privacidad en el manejo automatizado o manual de datos personales. En términos generales, el sujeto podrá ejercer: a) *derecho de acceso* a la información nominativa personal en los diversos bancos de datos; b) *derecho de información* sobre el uso, destino y duración del archivo de datos personales. En los casos del *habeas impropio* se utilizará el *habeas data* para el acceso a la información pública; c*) derecho de rectificación o actualización* de la información personal; d) *derecho de reserva*, tratándose de datos que son legítimamente recopilados pero cuyo acceso sea restringido, pudiendo ser conocido sólo por aquellos legalmente autorizados. Este derecho se relaciona con el manejo de la información sensible para cuyo manejo existen determinadas previsiones específicas”[213].

En el caso del habeas impropio (que se estudiará más adelante), esta tutela el derecho de conocer cierta información que no necesariamente es nuestra. En México, este es conocido como el derecho de acceso a la información pública.

3.6 Tipos de Hábeas Data.

Para comprender mejor cómo funciona el Habeas Data, y la manera en la que se puede usar, es necesario una clasificación para identificar rápidamente qué mecanismo o tipo de Habeas Data es eficaz usar de acuerdo con las circunstancias en particular. Es así como el Habeas Data se clasifica principalmente de acuerdo con el objetivo que persigue. Desde un de punto general, el Habeas Data tutela los derechos ARCO.

De manera general este trabajo de investigación considera adecuado usar la siguiente clasificación propuesta por SAGUÉS:

[213] Muñoz de Alba Medrano, Marcia. Habeas data. Consultado el 16 de marzo de 2023. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/5/2264/4.pdf

a) *"habeas data informativo*: cuando se utilice para obtener la información nominativa determinada, reglamentado en las Constituciones de Argentina, Brasil, Colombia, Ecuador, Guatemala, Paraguay y Perú;
b) *habeas data aditivo*, aquel que trata de actualizar o incluir datos o información dentro de los archivos, regulado en las Constituciones de Argentina, Brasil, Colombia, Ecuador y Paraguay;
c) *habeas data rectificador o correctivo* cuyo objetivo es corregir informaciones falsas, inexactas o imprecisas, regulado en las Constituciones de Argentina, Brasil, Colombia, Ecuador, Guatemala y Paraguay;
d) *habeas data reservador*, tiene por objeto asegurar que un dato determinado sea proporcionado a quienes se encuentran legalmente autorizados para conocerlo;
e) *habeas exclutorio* o *cancelatorio*: se trata de eliminar información almacenada en algún banco de datos o sistema de información, tiene relevancia para aquella información considerada como sensible, regulado en las Constituciones de Argentina, Ecuador y Paraguay"[214].

El resumen de los distintos tipos de *habeas data* recuperados por Sagués, se proporciona de manera ilustrativa más no limitativa. Este capítulo demuestra además que algunos países sí incluyen dentro de sus constituciones al habeas data como un derecho de rango constitucional. Sin embargo, en algunos países no se contempla de manera explícita la figura del Habeas Data, pero sí la protección jurídica de los datos personales y de la privacidad mediante algunas otras figuras jurídicas, como el amparo en el caso mexicano. Además, en la constitución mexicana se contemplan los derechos ARCO, los cuales se ejercen principalmente de manera directa ante un ente público o privado, todo esto siguiendo los lineamientos que establece la ley. Al respecto, estos mecanismos se tratarán en el siguiente capítulo.

[214] Cit. Por Muñoz de Alba Medrano, Marcia. Habeas Data. RU jurídicas. Repositorio Universitario. UNAM. Consultado el 28 de marzo de 2023. Disponible en:
http://ru.juridicas.unam.mx/xmlui/handle/123456789/26599
También referenciado en Torres, R. (2022). Régimen jurídico de la transparencia y acceso a la información pública gubernamental, datos personales y big data. [Tesis de maestría, Universidad Nacional Autónoma de México]. Repositorio institucional de la Universidad Nacional Autónoma de México.
http://132.248.9.195/ptd2022/diciembre/0833896/Index.html

Sea el habeas data un derecho o mecanismo judicial, sea recurrida o no con este nombre, su implementación es crucial para cualquier país. Además, cabe resaltar la importancia de que existan Leyes o Convenios por regiones, varios países, o zonas económicas estratégicas, que logren unificar la diversidad de conceptos, tipos y subtipos de habeas data o de mecanismos jurídicos que permita respetar la privacidad y salvaguardar los datos personales. Sobre todo porque en un plano internacional como lo es el ciberespacio, puede resultar complicado saber con exactitud qué tipo de norma aplicar, y la competencia jurisdiccional que resolverá determinado asunto.

CAPÍTULO IV. MARCO JURÍDICO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES Y DERECHO A LA PRIVACIDAD EN MÉXICO

4.1 Legislación mexicana en materia de protección de datos personales

El estudio de la protección de datos personales comienza a partir de la Segunda Guerra mundial al declararse distintos instrumentos internacionales en materia de derecho a la vida privada. En México, como tal, el derecho a la protección de los datos privados comenzó a desarrollarse con la doctrina que proporcionaba Europa y también con los esquemas de autorregulación que existían principalmente en Estados Unidos de América.

La primera ley que reconocía este derecho de protección de datos fue la Ley Federal de Acceso a la Información Pública Gubernamental de 2002, en la cual se reconoce el derecho de protección de datos en el ámbito público. Posteriormente, en 2009, las reformas constitucionales de los artículos 16 y 73 otorgaron el reconocimiento pleno a la protección de datos personales como un derecho fundamental y autónomo. Asimismo, estas reformas dotaron de facultades al Congreso de la Unión para legislar en la materia[215].

A pesar de que Ley Federal de Acceso a la Información Pública Gubernamental de 2002 comenzaba a mencionar la protección de datos personales, era claro que no era suficiente porque solo mencionaba algunos supuestos para la protección de los datos, pero no abarcaba los hoy conocidos derechos de acceso, rectificación cancelación u oposición (ARCO). Además, no existía ninguna legislación que protegiera a las personas frente a los particulares. En este sentido, en el 2010 se decreta la Ley Federal de Protección de Datos Personales en Posesión de Particulares, y en el 2017, se decreta la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en las cuales, se agregan los famosos derechos ARCO, se establecen los principios rectores de la materia, así como un procedimiento de verificación de cumplimiento de la

[215] Mendoza Enríquez, Olivia Andrea. 2018. Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. Instituto de Ciencias Jurídicas de Puebla. Revista IUS, vol. 12, núm. 41, pp.267-291. Consultado el: 25 de abril de 2023. Disponible en: https://www.redalyc.org/journal/2932/293258387015/html/

ley, se crearon los recursos jurídicos para hacer valer el derecho de protección de datos, se contemplan las sanciones para aquellos responsables que hicieran mal uso de los datos personales, se estableció por primera vez en México acerca del tratamiento transfronterizo, entre otros temas relacionados.

Las normas de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y otras normas más se analizan en este capítulo.

a) Constitución Política de los Estados Unidos Mexicanos.

La protección de los datos personales como derecho fundamental, se estipula en el artículo 6º constitucional, en su inciso A, y diversos incisos, que a la letra estipula:

> "*Fracción II: La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes."*
>
> *Fracción III*: *Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos*."[216]

Así mismo, en este artículo se estipula la base legal para el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

> Fracción 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*."[217]

[216] Constitución Política de los Estados Unidos Mexicanos. Consultado el 16 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf
[217] *Idem*.

Por su parte el artículo 16º constitucional además de contemplar la protección a los datos personales, se establecen los derechos ARCO, siendo este artículo la base de la Ley Federal de Protección de Datos Personales en Posesión de Particulares:

> Art. 16 "…*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*."[218]

Una vez que se conocen las bases para la creación de las principales leyes en materia de protección de datos personales, se analizan en este capítulo la Ley Federal de Protección de Datos Personales en Posesión de Particulares (así como su reglamento, la cual es analizada dentro del apartado de su Ley) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

4.2 Análisis de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

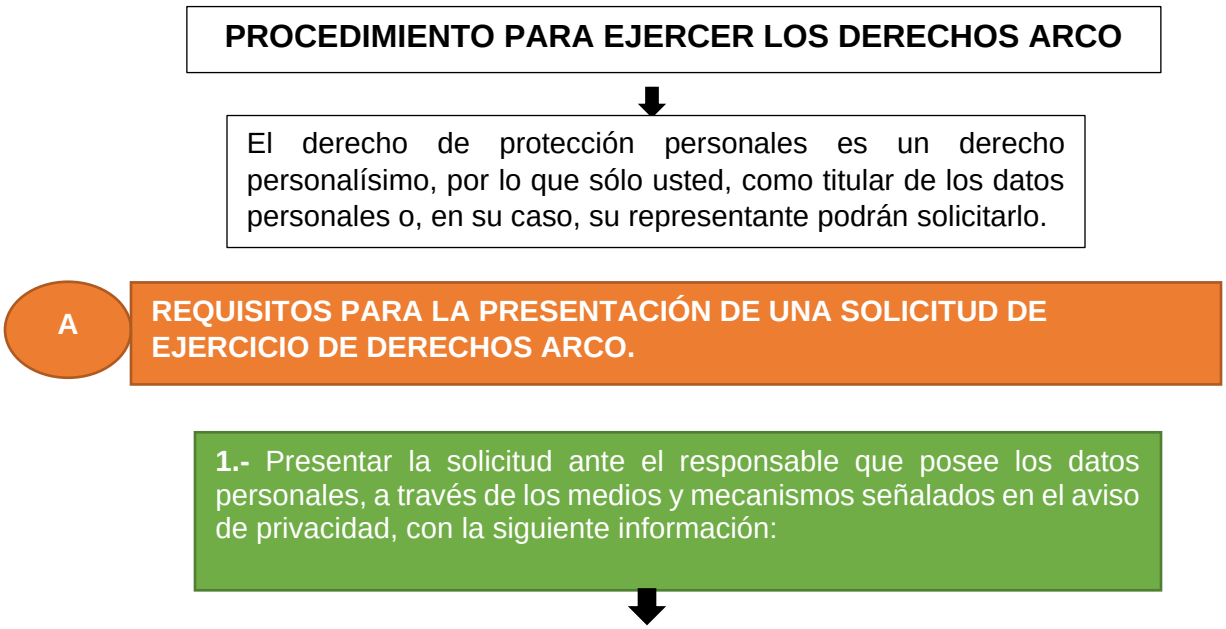
La Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) tiene por objeto proteger los datos personales y los datos sensibles de las personas que residen en territorio mexicano, frente a cualquier particular que trate sus datos, sea este un tratamiento físico o digital; en territorio mexicano o en el extranjero, esto con el fin de garantizar el ejercicio del derecho de autodeterminación informativa y a la vida privada.

En primer término, esta ley estable que desde el aviso de privacidad los responsables encargados del tratamiento de datos personales deben de establecer dentro de dicho aviso de privacidad los medios para ejercer los derechos ARCO, así como las opciones y los medios que el responsable ofrezca a los titulares para limitar el uso o divulgación

[218] *Idem*.

de sus datos, sin embargo, todavía existen particulares que de manera física o digital recaban datos personales y no proporcionan ningún tipo de aviso de privacidad. Dejando en desventaja a los titulares de los datos personales por no saber cómo ejercer sus derechos ARCO. A juicio de la suscrita, es sumamente importante que de primera mano los responsables sean el primer enlace para atender cualquier solicitud de acceso, rectificación, cancelación u oposición. Sólo así se puede resolver de manera rápida, eficiente y expedita cualquier vulneración que presente el titular con sus datos personales.

En caso de que el responsable del tratamiento de datos personales no proporcione ningún medio de defensa al titular de los datos, la LFPDPPP a partir de su artículo 28 y artículo 87 del Reglamento de dicha ley establecen cómo serán las solicitudes de ejercicio de derechos ARCO, el cual el responsable del tratamiento deberá dar respuesta a la solicitud del titular en un plazo máximo de veinte días contados a partir de la fecha en la que se recibió la solicitud. Así mismo, el INAI estableció a través de su página web las instrucciones para hacer una solicitud de derechos ARCO. Para fines prácticos se adjunta dichas instrucciones:



Información general:

- Nombre del titular de los datos personales.
- Documentos que acrediten la identidad del titular.
- En su caso, nombre del representante del titular y documentos para acreditar su identidad y personalidad.
- Domicilio o cualquier medio para recibir notificaciones.
- Descripción clara y precisa de los datos personales que se quieran rectificar, cancelar u oponerse a su tratamiento.
- Descripción del derecho que se quiere ejercer o de lo que solicita el titular.
- En su caso, documentos o información que faciliten la localización de los datos personales, entre ella, el área responsable del tratamiento.

Información específica: esta depende del derecho ARCO que se pretende ejercer.

- Derecho de **ACCESO:** la modalidad en la que prefiere que se reproduzcan los datos personales solicitados.
- Derecho de **RECTIFICACIÓN:** las modificaciones que solicita que se realicen a los datos personales, así como aportar los documentos que sustenten la solicitud.
- Derecho de **CANCELACIÓN:** las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.
- Derecho de **OPOSICIÓN:** las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

Cuando presente su solicitud, el responsable le deberá entregar un ACUSE en el que conste la fecha de recepción de la misma.

REQUERIMIENTO

Si la solicitud no tiene toda la información descrita, el responsable puede solicitar la información faltante a través de un requerimiento el cual se deberá emitir en un plazo máximo de 5 días hábiles contados a partir del día siguiente de la presentación de la solicitud, y usted tendrá 10 días hábiles, después de recibir la prevención, para proporcionar la información requerida, pues de lo contrario se tendrá como no presentada su solicitud.

2.- Acreditar la identidad del titular y, en su caso, la de su representante, así como la personalidad de este último.

La solicitud se deberá de acompañar de copia simple de una identificación oficial de usted como titular de los datos personales, así como de su representante, en caso de que sea éste quien presente la solicitud.

3. Tomar en cuenta las siguientes reglas de representación en caso de solicitudes relacionadas con datos personales de menores de edad, personas en estado de interdicción o incapacidad declarada por ley.

Menores de edad

1 Padres

1.-Documento que acredite la identidad de menor.
2.-Acta de nacimiento del menor.
3.-Identificación oficial del padre o de la madre, que pretenda ejercer el derecho.
4.-Carta en la que se manifieste, bajo protesta de decir verdad, que el padre o la madre es quien ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

2 Persona distinta a los padres

1.- Los documentos del punto 1 y 2 de la primera columna.
2.-Documento legal que acredite la posesión de la patria potestad.
3.-Identificación oficial de quien presenta la solicitud y posee la patria potestad.
4.-Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

3 Tutor

•1.- Los documentos del punto 1 y 2 de la primera columna
2.-Documento legal que acredite la tutela.
3.-Identificación oficial del tutor.
4.-Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la tutela.

Personas en estado de interdicción o incapacidad legal

- Documento que acredite la identidad del titular de los datos personales.
- Instrumento legal de designación del tutor.
- Identificación oficial del tutor.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de lo alguno de los supuestos legales de suspensión o limitación de la misma.

B **PLAZOS Y PROCEDIMIENTO PARA LA ATENCIÓN DE LAS SOLICITUDES DE EJERCICIO DE DERECHOS ARCO**

Una vez que se presentó la solicitud y que ésta cumplió con los requisitos antes descritos, el responsable ante el cual se presentó deberá realizar lo siguiente:

En un plazo de **20 días hábiles**, contados a partir del día siguiente a la recepción de la solicitud, deberá informarle si procede o no el ejercicio del derecho solicitado.

En caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo, en un plazo de **15 días hábiles**, contados a partir del día siguiente en el que le haya notificado la respuesta anterior.

- Los plazos antes señalados se pueden ampliar por un periodo igual, cuando esté justificado y se le informe de ello. En caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo, en un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior.
- El ejercicio de los derechos ARCO será sencillo y **GRATUITO**, sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación de documentos o envío de información.
- cuando las disposiciones aplicables a determinadas bases de datos o tratamientos establezcan un procedimiento específico para solicitar el ejercicio de los derechos ARCO, se estará a lo dispuesto en aquéllas que ofrezcan mayores garantías al titular, y no contravengan las disposiciones previstas en la Ley.

Fuente: elaboración propia con los requisitos proporcionados en la página web del INAI. https://home.inai.org.mx/?page_id=3374

Ahora bien, cuando el responsable del tratamiento de los datos personales no dé ninguna respuesta en la solicitud de derecho ARCO, el titular puede iniciar un procedimiento de protección de datos personales el cual será resuelto por el INAI. Dicho formato para presentar la solicitud es la siguiente:

SOLICITUD DE PROTECCIÓN DE DERECHOS

FORMATO PARA SOLICITAR LA PROTECCIÓN DEL INAI POR INCUMPLIMIENTO DEL RESPONSABLE CON MOTIVO DEL EJERCICIO DE LOS DERECHOS DE LOS TITULARES
ANTES DE REQUISITAR EL PRESENTE FORMATO, FAVOR DE LEER EL INSTRUCTIVO DE LLENADO AL REVERSO.
LOS ESPACIOS QUE CONTENGAN * SÓLO DEBERÁN SER LLENADOS EN CASO DE QUE LE SEAN APLICABLES.

1 FOLIO: _____

2 _____ UNIDAD RECEPTORA

3 _____ FECHA (DD/MM/AA)

4 DATOS DEL TITULAR

APELLIDO PATERNO | APELLIDO MATERNO | NOMBRE(S)

DOMICILIO:

CALLE | NÚMERO EXTERIOR – INTERIOR | COLONIA

POBLACIÓN | DELEGACIÓN O MUNICIPIO | ENTIDAD FEDERATIVA | C.P.

TELÉFONO | CORREO ELECTRÓNICO

5 DATOS DEL RESPONSABLE

NOMBRE O DENOMINACIÓN SOCIAL

DOMICILIO:

CALLE | NÚMERO EXTERIOR – INTERIOR | COLONIA

POBLACIÓN | DELEGACIÓN O MUNICIPIO | ENTIDAD FEDERATIVA | C.P.

TELÉFONO | CORREO ELECTRÓNICO

6 DATOS DEL DERECHO EJERCIDO

TIPO DE DERECHO: ACCESO ☐ RECTIFICACIÓN ☐ CANCELACIÓN ☐ OPOSICIÓN ☐

LA SOLICITUD DE EJERCICIO SE REFIERE A DATOS PERSONALES SENSIBLES: SI ☐ NO ☐

FECHA DE PRESENTACIÓN DE LA SOLICITUD ARCO ANTE EL RESPONSABLE (DD/MM/AA) | * FECHA DE RESPUESTA DEL RESPONSABLE A LA SOLICITUD ARCO (DD/MM/AA) | * MEDIO A TRAVÉS DEL CUAL SE DIO A CONOCER LA RESPUESTA

ESCRITO ☐

CORREO ELECTRÓNICO ☐

7 SEÑALE CON CLARIDAD EL O LOS MOTIVOS DE SU RECLAMACIÓN Y, EN SU CASO, LOS PRECEPTOS DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES QUE CONSIDERE LE FUERON VULNERADOS

8	MEDIO A TRAVÉS DEL CUAL SE LE HARÁN LAS NOTIFICACIONES

MEDIOS DE COMUNICACIÓN ELECTRÓNICA (ART. 35, DE LA LEY FEDERAL DE PROCEDIMIENTO ADMINISTRATIVO) ☐ _____ INDICAR CORREO ELECTRÓNICO CORREO CERTIFICADO CON ACUSE DE RECIBO ☐

DOMICILIO PARA OÍR Y RECIBIR NOTIFICACIONES (SÓLO SI DESEA QUE LAS NOTIFICACIONES SE LE HAGAN VÍA CORREO CERTIFICADO)

CALLE | NÚMERO EXTERIOR – INTERIOR | COLONIA

POBLACIÓN | DELEGACIÓN O MUNICIPIO | ENTIDAD FEDERATIVA | C.P.

EL TITULAR CUENTA CON FIRMA ELECTRÓNICA AVANZADA (FIEL) EXPEDIDA POR EL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA (SAT) SI ☐ NO ☐

* NOMBRE DEL REPRESENTANTE LEGAL DEL TITULAR: _____

DOMICILIO DEL REPRESENTANTE LEGAL PARA OÍR Y RECIBIR NOTIFICACIONES (SÓLO SI DESEA QUE LAS NOTIFICACIONES SE LE HAGAN VÍA CORREO CERTIFICADO)

CALLE | NÚMERO EXTERIOR – INTERIOR | COLONIA

POBLACIÓN | DELEGACIÓN O MUNICIPIO | ENTIDAD FEDERATIVA | C.P.

EL REPRESENTANTE LEGAL CUENTA CON FIRMA ELECTRÓNICA AVANZADA (FIEL) EXPEDIDA POR EL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA (SAT) SI ☐ NO ☐

9	DOCUMENTOS QUE SE DEBEN ADJUNTAR A LA SOLICITUD

a) COPIA DE LA SOLICITUD DEL EJERCICIO DE DERECHOS, CON SU CORRESPONDIENTE ACUSE DE RECIBIDO POR PARTE DEL RESPONSABLE
b) EL DOCUMENTO CON EL QUE SE ACREDITE LA RESPUESTA, QUE, EN SU CASO, HUBIERE DADO EL RESPONSABLE
c) DOCUMENTO DE IDENTIFICACIÓN Y COPIA PARA SU COTEJO
d) DOCUMENTO CON EL QUE SE ACREDITA LA REPRESENTACIÓN*
e) LA(S) PRUEBA(S) DOCUMENTAL(ES) QUE OFRECE PARA DEMOSTRAR SU(S) AFIRMACION(ES)
f) EL DOCUMENTO EN EL QUE SEÑALE LAS DEMÁS PRUEBAS QUE OFREZCA
g) CUALQUIER DOCUMENTO QUE CONSIDERE PROCEDENTE SOMETER A JUICIO DEL INSTITUTO

10	MANIFIESTA SU VOLUNTAD DE PARTICIPAR EN AUDIENCIA(S) CONCILIATORIA(S) CON EL RESPONSABLE, CON EL OBJETO DE OBTENER UNA SOLUCIÓN ÁGIL Y EFICAZ A SU RECLAMACIÓN

SI ☐ NO ☐

11	OBSERVACIONES

BAJO PROTESTA DE DECIR VERDAD MANIFIESTO QUE LOS DATOS ASENTADOS EN EL PRESENTE SON CIERTOS, INCLUYENDO LOS QUE ACREDITAN LA IDENTIDAD DEL TITULAR.

_____

NOMBRE Y FIRMA DEL TITULAR O DE SU REPRESENTANTE LEGAL

INSTRUCTIVO DE LLENADO		
1	FOLIO	CORRESPONDE AL NÚMERO ÚNICO CONSECUTIVO QUE ASIGNARÁ EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI) A LA SOLICITUD PARA SU CONTROL.
2	UNIDAD RECEPTORA	ESTE DATO SERÁ INCORPORADO POR EL INSTITUTO PARA EFECTOS DE CONTROL INTERNO.
3	FECHA	ES EL DÍA, MES Y AÑO EN QUE SE PRESENTA LA SOLICITUD.
4	DATOS PERSONALES DEL TITULAR	DEBERÁS SEÑALAR TU NOMBRE COMPLETO CON EL OBJETO DE QUE ESTÉS PLENAMENTE IDENTIFICADO (A) EN EL PROCEDIMIENTO LEGAL QUE VAS A INICIAR ANTE EL INAI. DOMICILIO: ES EL QUE SEÑALES PARA OÍR Y RECIBIR TODA LA INFORMACIÓN QUE EL INAI TENGA QUE DARTE A CONOCER CON RELACIÓN AL PROCEDIMIENTO. ES IMPORTANTE QUE SEÑALES UN TELÉFONO Y UNA DIRECCIÓN DE CORREO ELECTRÓNICO, EN CASO DE QUE CUENTE CON ELLOS, PARA EFECTO DE FACILITAR CUALQUIER INFORMACIÓN QUE SE TE QUIERA DAR A CONOCER.
5	DATOS DEL RESPONSABLE	ES QUIEN DECIDE SOBRE LA OBTENCIÓN, USO, DIVULGACIÓN O ALMACENAMIENTO DE TUS DATOS Y A QUIEN DIRIGISTE LA SOLICITUD DE EJERCICIO DE DERECHOS ARCO (ACCESO, RECTIFICACIÓN, CANCELACIÓN U OPOSICIÓN) O DE REVOCACIÓN DEL CONSENTIMIENTO. ESTA INFORMACIÓN ES INDISPENSABLE A FIN DE QUE EL INAI SE ENCUENTRE EN POSIBILIDAD DE NOTIFICAR O UBICAR AL RESPONSABLE.
6	DATOS DEL DERECHO EJERCIDO	SE RELACIONAN CON EL TIPO DE SOLICITUD DE EJERCICIO DE DERECHOS "ARCO" QUE EL TITULAR O SU REPRESENTANTE PRESENTÓ ANTE EL RESPONSABLE; DEBERÁ SEÑALAR EL SUPUESTO EN QUE ENCUADRA SU RECLAMACIÓN: a. ACCESO A LOS DATOS PERSONALES DEL TITULAR.- ES TU DERECHO PARA SOLICITAR Y CONOCER SI TU INFORMACIÓN PERSONAL ESTÁ SIENDO OBJETO DE TRATAMIENTO Y LAS CONDICIONES DE ÉSTE. b. RECTIFICACIÓN.- ES EL DERECHO QUE TIENES PARA QUE SE CORRIJAN TUS DATOS PERSONALES O COMPLETARLOS CUANDO SEAN INEXACTOS O INCOMPLETOS. c. CANCELACIÓN (ELIMINACIÓN).- ES TU DERECHO A SOLICITAR LA SUPRESIÓN O ELIMINACIÓN DE TUS DATOS PERSONALES DE UN SISTEMA DE DATOS PERSONALES CUANDO CONSIDERES QUE LOS MISMOS NO ESTÁN SIENDO TRATADOS CONFORME A LOS PRINCIPIOS, DEBERES Y OBLIGACIONES PREVISTOS EN LA LEY. d. OPOSICIÓN.- ES EL DERECHO QUE TIENES DE SOLICITAR EL CESE DEL TRATAMIENTO DE TUS DATOS PERSONALES POR LAS SIGUIENTES RAZONES: CUANDO EXISTA UNA CAUSA LEGÍTIMA DERIVADA DE TU PROPIA SITUACIÓN PERSONAL; CUANDO LO DETERMINES POR UNA FINALIDAD ESPECÍFICA. e. REVOCACIÓN.- EN ESTE APARTADO, TAMBIÉN PODRÁS SEÑALAR SI EL DERECHO QUE EJERCISTE ANTE EL RESPONSABLE, FUE EL DE MANIFESTAR TU DESEO PARA QUE DICHO RESPONSABLE YA NO TRATE TUS DATOS PERSONALES. SE ENTIENDE POR DATOS SENSIBLES AQUELLOS QUE AFECTEN A LA ESFERA MÁS ÍNTIMA DE UNA PERSONA, TALES COMO ORIGEN RACIAL O ÉTNICO, ESTADO DE SALUD, INFORMACIÓN GENÉTICA, CREENCIAS RELIGIOSAS, FILOSÓFICAS Y MORALES, AFILIACIÓN SINDICAL, OPINIONES POLÍTICAS, PREFERENCIA SEXUAL. . ASIMISMO, DEBERÁS PRECISAR EL DÍA, MES Y AÑO EN QUE PRESENTASTE LA SOLICITUD DE EJERCICIO DE DERECHOS "ARCO" ANTE EL RESPONSABLE O EN QUE SOLICITASTE LA REVOCACIÓN, LA CUAL DEBE CORRESPONDER CON AQUELLA QUE CONSTE EN EL ESCRITO RESPECTIVO; IGUALMENTE, EL DÍA, MES Y AÑO EN QUE ÉSTE DIO RESPUESTA (SÓLO EN CASO DE QUE LA HUBIERA DADO) Y EL MEDIO A TRAVÉS DEL CUAL SE DIO A CONOCER DICHA RESPUESTA (YA SEA POR ESCRITO O POR CORREO ELECTRÓNICO).
7	ACTOS QUE MOTIVAN LA SOLICITUD	DEBERÁS EXPLICAR BREVEMENTE LAS CAUSAS POR LAS CUALES SOLICITAS LA INTERVENCIÓN DEL INSTITUTO. ASÍ COMO SEÑALAR CUALQUIER CIRCUNSTANCIA QUE CONSIDERES IMPORTANTE PARA ELLO.
8	MEDIO A TRAVÉS DEL CUAL SOLICITA SE LE HAGAN LAS NOTIFICACIONES.	DEBERÁS SEÑALAR EL MEDIO A TRAVÉS DEL CUAL SOLICITAS QUE EL INSTITUTO TE INFORME TODO LO RELATIVO AL PROCEDIMIENTO QUE INICIAS, YA SEA POR EL SISTEMA ELECTRÓNICO DEL INAI O POR CORREO CERTIFICADO UTILIZANDO EL SERVICIO POSTAL MEXICANO (SEPOMEX); EN ESTE ÚLTIMO CASO DEBERÁS SEÑALAR UN DOMICILIO PARA OÍR Y RECIBIR NOTIFICACIONES, QUE SE ENCUENTRE UBICADO EN TERRITORIO NACIONAL, CONFORME A LO SEÑALADO EN EL NUMERAL 4.
9	DOCUMENTOS QUE SE DEBEN ADJUNTAR	LA SOLICITUD PRESENTADA AL RESPONSABLE, DEBERÁ MOSTRAR EL ACUSE DE RECIBIDO, YA SEA EN LA MISMA SOLICITUD O EN DOCUMENTO SEPARADO. SI TE ES POSIBLE, ANEXA EL DOCUMENTO QUE PRESENTASTE ANTE EL RESPONSABLE PARA ACREDITAR TU IDENTIDAD PERO RECUERDA QUE EL INSTITUTO TE PUEDE REQUERIR ALGÚN OTRO DOCUMENTO PARA ELLO. LOS DOCUMENTOS OFICIALES PARA ACREDITARTE PODRÁN SER: CREDENCIAL DEL IFE, PASAPORTE, CARTILLA DEL SERVICIO MILITAR NACIONAL, CÉDULA PROFESIONAL, CARTILLA DE IDENTIDAD POSTAL EXPEDIDA POR EL SERVICIO POSTAL MEXICANO. ADEMÁS DE ESTOS DOCUMENTOS, SE CONSIDERARÁN COMO TALES, INDISTINTAMENTE, EL CERTIFICADO O CONSTANCIA DE ESTUDIOS, CONSTANCIA DE RESIDENCIA EMITIDA POR LA AUTORIDAD DEL LUGAR DE RESIDENCIA DEL TITULAR O CREDENCIAL DE AFILIACIÓN DEL INSTITUTO MEXICANO DEL SEGURO SOCIAL O DEL INSTITUTO DE SEGURIDAD Y SERVICIOS SOCIALES DE LOS TRABAJADORES DEL ESTADO. EN CASO DE QUE PROMUEVAS A TRAVÉS DE UN REPRESENTANTE, DEBERÁS ANEXAR EL INSTRUMENTO DEL NOTARIO PÚBLICO O LA CARTA PODER ANTE DOS TESTIGOS, EN QUE CONSTA DICHA REPRESENTACIÓN. TRATÁNDOSE DE MENORES DE EDAD O INCAPACES, DEBERÁS ANEXAR COPIA CERTIFICADA DEL ACTA DE NACIMIENTO O COPIA CERTIFICADA DE LA DESIGNACIÓN DE TUTOR, RESPECTIVAMENTE. SI ERES DE NACIONALIDAD EXTRANJERA, ES NECESARIO QUE ADJUNTES EL ORIGINAL O COPIA CERTIFICADA DE TU DOCUMENTO MIGRATORIO VIGENTE. ES NECESARIO QUE EL DOCUMENTO QUE ACREDITE TU IDENTIDAD COMO TITULAR O REPRESENTANTE, SEA VIGENTE O ACTUALIZADO. ADICIONALMENTE A LOS DOCUMENTOS ANTES SEÑALADOS, DEBERÁS ANEXAR A TU SOLICITUD LOS DEMÁS DOCUMENTOS CON QUE CUENTES PARA ACREDITAR TU DERECHO Y OFRECER LAS PRUEBAS QUE CONSIDERES NECESARIO PARA ELLO, TALES COMO PERICIAL, TESTIMONIAL O LA DE INSPECCIÓN. **SE TE RECUERDA QUE DEBERÁS ADJUNTAR A TU SOLICITUD, ADEMÁS, UNA COPIA DE TODA LA DOCUMENTACIÓN QUE ENTREGUES AL INAI, PARA EFECTOS DE ENTREGÁRSELA AL RESPONSABLE CUANDO SE LE NOTIFIQUE.**
10	MANIFESTACIÓN DE VOLUNTAD PARA CONCILIAR	DEBERÁS MANIFESTAR SI ESTÁS DE ACUERDO O NO EN PARTICIPAR EN UN MECANISMO CONCILIACIÓN CON EL RESPONSABLE.
11	OBSERVACIONES	PODRÁS ANOTAR AQUELLOS COMENTARIOS ADICIONALES QUE ESTIMES PERTINENTE FORMULAR.

NOTA: SE HACE DEL CONOCIMIENTO DEL TITULAR QUE SUS DATOS PERSONALES RECABADOS EN EL PRESENTE FORMATO SERÁN TRATADOS POR EL INAI CON LA FINALIDAD DE ATENDER EL PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS PREVISTO EN EL CAPÍTULO VII DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. ASIMISMO, CON FUNDAMENTO EN LO PREVISTO POR EL ARTÍCULO 113 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, Y AL ARTÍCULO 110 FRACCIONES VI Y XI, DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, EL EXPEDIENTE DEL PROCEDIMIENTO ADMINISTRATIVO QUE CORRESPONDA A LA PRESENTE SOLICITUD DE PROTECCIÓN DE DERECHOS, SERÁ CONSIDERADO COMO INFORMACIÓN RESERVADA EN TANTO NO HAYA QUEDADO FIRME LA RESOLUCIÓN QUE EN ÉL SE EMITA.

PARA CUALQUIER DUDA O COMENTARIO ESTÁN A TU DISPOSICIÓN LOS SIGUIENTES MEDIOS:
TELÉFONO: 01 800 TELINAI (01 800 8354324) CORREO ELECTRÓNICO: atención@inai.org.mx

Fuente: https://home.inai.org.mx/wp-content/documentos/formatos/PDP/SolicitudPD.pdf

Si bien esta ley fue muy novedosa en su momento, en la actualidad no es suficiente para garantizar una eficaz protección de los datos personales y de la vida privada de las personas, porque hoy en día, la mayoría de los tratamientos de datos personales no se realizan solo de manera física, se realiza más bien en un mundo digital e internacional. Desde el punto de vista de la suscrita, esta LFPDPPP tiene diversos artículos que adecuar, por lo tanto, este apartado también lo destino como un espacio de análisis.

La Ley establece en su artículo 2 quienes son los sujetos regulados, mencionando que son las personas físicas o morales (llamadas ahora jurídico-colectivas), con excepción de aquellas sociedades de información crediticia, lo cual, a punto de vista de la sustentante, el o la legislador tiene que unificar el criterio de observancia legal, estableciendo una ley que regule a cualquier ente privado que trate datos personales, sean cualquiera que sea su giro de negocio o de actividades. Al unificar este criterio de sujetos obligados, facilitaría muchísimo para las personas el saber cómo proteger sus datos personales. Con esto, no pretendo dar a entender que la Ley para Regular las Sociedades de Información Crediticia y las instituciones que se sujetan a esa Ley deba desaparecer, simplemente la idea en general es que estas sociedades no deben de estar exceptuadas a los principios y lineamientos mínimos de protección de datos personales de la LFPDPPP y del resto de los instrumentos jurídicos que México ya ratificó.

Otro aspecto para tomar a cuenta es que el artículo 4 de la LFPDPPP establece que "*Los principios y derechos previstos en esta Ley, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros*"[219], en el cual, se requiere más especificidad para comprender cuál es el límite que abarca proteger dicha seguridad nacional, el orden, la seguridad y la salud pública. Si por alguna cuestión no se puede incluir en la ley, deben existir pautas o lineamientos que sean vinculantes y no sólo documentos de recomendación. Esto es esencial porque como se expuso en el capítulo II, hoy en día los Estados destinan las tecnologías de la información y el procesamiento

[219] Artículo 4 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Consultado el 12 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

de datos para crear perfiles que de acuerdo con su criterio determinan quién o quiénes son personas “potencialmente peligrosas” para el Estado. Estos casos ya sucedieron en México, en donde por ejemplo la Secretaría de la Defensa Nacional fue hackeada por un grupo de hacktivistas los cuales dieron a conocer que la SEDENA tenía bases de datos que apuntaban a los activistas por los derechos de las mujeres (y no se duda que aún las tenga) como personas peligrosas. Existen otros países que de manera más exagerada recopilan los datos persona de sus ciudadanos y clasifican su estilo de vida, creando tipos de perfiles que determinan cómo será la vida de esas personas, como lo es el caso de China.

Por ello, es esencial que los legisladores y legisladores se ocupen de definir los alcances y límites de estas excepciones que se dan en caso de proteger la seguridad nacional, el orden, la seguridad y la salud pública. Además, se requiere que como sociedad mexicana se tenga un pleno conocimiento sobre el poder que tienen los datos personales de cada uno/a.

Por lo que se refiere al tema del consentimiento, este se debe de adecuar a las exigencias que presenta hoy en día dentro del mundo digital. Las leyes de protección de datos deben de exigir que cualquier sujeto, sea este público o privado, proporcione los medios necesarios para recabar de manera directa el consentimiento del titular de los datos personales, a través de los famosos “avisos de privacidad”, y que las personas usuarias de sus servicios o compra de bienes, puedan elegir qué datos se pueden recabar de su relación comercial, médica, social, etc., esto de mano con las famosas *cookies* (para el caso de alguna relación que involucra el internet) o mediante formatos físicos (para el caso de tratamientos físicos y directos).

En la actualidad existen varias páginas, sitios web o plataformas en internet que ya incluyen estos famosos avisos de privacidad, garantizando así a los titulares de los datos el derecho de autodeterminación informativa, pero también existen muchos responsables del tratamiento de datos que no incluyen ningún tipo de aviso de privacidad (física o digital).

A mi criterio, el tema del consentimiento es uno de los temas más importantes (si no es que el más importante) para garantizar una correcta protección a los datos personales y

a la vida privada, pues como se mencionó en repetidas ocasiones, a partir del consentimiento es como se va a regir cualquier relación jurídica. Entonces, cuando se proporciona de manera adecuada, concreta y sencilla toda la información concerniente al cómo, cuándo, y quién tratará los datos personales, el titular de estos sabe con certeza que el responsable no le dará otro uso fuera de la finalidad para el tratamiento de datos.

En relación con el tratamiento de datos personales sensibles, la ley estipula que "*Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca*"[220], redacción que a primera vista parece correcta, sin embargo, estipular que *"cualquier mecanismo de autenticación que al efecto se establezca*" es suficiente para tratar datos personales es una equivocación. Hoy en día, cuando las personas navegan en un ambiente casi completamente digital, lo que más quieren es hacer las cosas rápido, para lo cual, no le dan la importancia debida a los términos y condiciones de un aviso de privacidad, por ello, como se mencionó anteriormente, la ley debe de ser más clara, específica y estricta en cuanto al tema del consentimiento, dado que estipular que *"cualquier mecanismo de autenticación que al efecto se establezca*" es suficiente para hacer legal un consentimiento que autorice datos personales sensibles da pauta a vacíos legales y puede permitir que los titulares de los datos no conozcan a profundidad el porqué del tratamiento de sus datos personales. A mi criterio sería correcto establecer que la sólo firma autógrafa o firma electrónica son por excelencia el medio de verificación para saber que un titular otorgó su consentimiento para tratar datos personales sensibles.

Al mismo tiempo, el artículo 18 de la LFPDPPP parece contener un vacío legal, pues se establece que el responsable podrá instrumentar medidas compensatorias para el caso en que el responsable vuelva a tratar los datos personales del titular y que el responsable no tenga ninguna manera de hacerle saber al titular el nuevo aviso de privacidad; el Reglamento de la Ley establece que estas medidas compensatorias de comunicación masiva seguirán los criterios establecidos por el Instituto Nacional de Transparencia,

[220] Artículo 9 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Consultado el 12 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Acceso a la Información Pública y Protección de Datos Personales (INAI), sin embargo, en ninguna parte de la Ley y del Reglamento se menciona cuáles y de qué tipo serán las medidas compensatorias, y tampoco establece algún tipo de lineamiento para que se establezcan esas medidas compensatorias, dejando al arbitrio del Instituto elegir cómo serán dichas medidas compensatorias sin tener lineamientos legales.

En cuanto al tema de las transferencias internacionales, el artículo 37 en su fracción IV de la multicitada Ley llama la atención, pues estipula que las transferencias internacionales de protección de datos personales se pueden dar sin el consentimiento del titular bajo distintos escenarios, y uno de ellos es cuando la transferencia sea necesaria por virtud de "…*un contrato por celebrar en interés del titular, por el responsable y un tercero"*[221]*,* para lo cual, la redacción tiene una laguna legal, pues puede servir de pauta para interpretarse como que el responsable puede transferir los datos del titular a un tercero cuando se crea que dicha transferencia puede posiblemente ser de interés benéfico al titular. El análisis de este artículo en particular resulta interesante, pues en el caso de una compañía multinacional que argumente transferir datos de titulares a un tercero puede argumentar que dicha transferencia es para el beneficio del titular, escondiendo de fondo intereses particulares presentes o futuros de dicha compañía.

El tema sobre la portabilidad de los datos personales es un tema que hace falta agregar a la LFPDPPP. Esta portabilidad, que sólo se contempla en la LGPDPPSO -en parte porque esta ley es más moderna- consiste en que cuando estos datos se encuentren en una base de datos computarizados en un formato estructurado el titular tiene el derecho de pedir al responsable del tratamiento de los datos a obtener una copia de sus datos personales tratados, esto en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. Como resultado de esta portabilidad de datos personales, Javier Martínez Cruz argumenta que "ejercer la portabilidad de los datos significa numerosos beneficios para la ciudadanía, ya que los propios titulares pueden

[221] Artículo 37 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Consultado el 12 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

obtener la información que han entregado a distintas instituciones y realizar los trámites que deseen, sin necesidad de que terceras personas accedan a ella"[222].

En diversos foros en materia de protección de datos personales y privacidad, se mencionó el principal reto que tiene México para actualizar la normativa de esta materia. Porque la LFPDPPP fue novedosa en su momento, pero con los rápidos avances de la tecnología, esta ley necesita hacerse efectiva e incluir pautas de regulación para el uso de los datos personales en la aplicación de la IA, en la neurociencia, y en general todo lo relacionado con la cuarta revolución industrial.

4.3 Análisis Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Para la materia de protección de datos personales en posesión de sujetos obligados, la LGPDPPSO, regula a todos los ámbitos de gobierno de los tres niveles, el federal, estatal y municipal, además de todos aquellos que para el ejercicio de sus funciones usen recursos públicos.

El ejercicio de protección de datos personales por los particulares se establece a partir del artículo 48 de la LGPDPPSO, en el cual, se estipula que el responsable debe de mencionar los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO. Aunque también existen sujetos obligados que no cuentan con ningún tipo de aviso de privacidad, a través de una solicitud de los derechos ARCO el titular de los datos puede hacer ejercicio de estos derechos. De igual manera que en la LFPDPPP y para efectos prácticos, el INAI proporciona los lineamientos a seguir para cualquier solicitud de derechos ARCO:

[222] Portabilidad de los datos personales beneficia a la ciudadanía. 2019. Infoem. Consultado el 27 de abril de 2023. Disponible en: https://www.infoem.org.mx/es/contenido/noticias/portabilidad-de-los-datos-personales-beneficia-la-ciudadan%C3%ADa#:~:text=Ejercer%20la%20portabilidad%20de%20los,ella%2C%20afirm%C3%B3%20Javier%20Mart%C3%ADnez%20Cruz

PROCEDIMIENTO PARA EJERCER LOS DERECHOS ARCO

El derecho de protección personales es un derecho personalísimo, por lo que sólo usted, como titular de los datos personales o, en su caso, su representante podrán solicitarlo.

A **REQUISITOS PARA LA PRESENTACIÓN DE UNA SOLICITUD DE EJERCICIO DE DERECHOS ARCO.**

1.- Presentar la solicitud ante el responsable que posee los datos personales, a través de los medios y mecanismos señalados en el aviso de privacidad, con la siguiente información:

Información general:

- Nombre del titular de los datos personales.
- Documentos que acrediten la identidad del titular.
- En su caso, nombre del representante del titular y documentos para acreditar su identidad y personalidad.
- Domicilio o cualquier medio para recibir notificaciones.

- Descripción clara y precisa de los datos personales que se quieran rectificar, cancelar u oponerse a su tratamiento.
- Descripción del derecho que se quiere ejercer o de lo que solicita el titular.
- En su caso, documentos o información que faciliten la localización de los datos personales, entre ella, el área responsable del tratamiento.

Información específica: esta depende del derecho ARCO que se pretende ejercer.

- Derecho de **ACCESO:** la modalidad en la que prefiere que se reproduzcan los datos personales solicitados.
- Derecho de **RECTIFICACIÓN:** las modificaciones que solicita que se realicen a los datos personales, así como aportar los documentos que sustenten la solicitud.
- Derecho de **CANCELACIÓN:** las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.
- Derecho de **OPOSICIÓN:** las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

Cuando presente su solicitud, el responsable le deberá entregar un ACUSE en el que conste la fecha de recepción de la misma.

PREVENCIÓN

Si la solicitud no tiene toda la información descrita, el responsable puede solicitar la información faltante a través de una prevención la cual se deberá emitir en un plazo máximo de 5 días hábiles contados a partir del día siguiente de la presentación de la solicitud, y usted tendrá 10 días hábiles, después de recibir la prevención, para proporcionar la información requerida, pues de lo contrario se tendrá como no presentada su solicitud.

2.- Acreditar la identidad del titular y, en su caso, la de su representante, así como la personalidad de este último.

La solicitud se deberá de acompañar de copia simple de una identificación oficial de usted como titular de los datos personales, así como de su representante, en caso de que sea éste quien presente la solicitud.

3. Tomar en cuenta las siguientes reglas de representación en caso de solicitudes relacionadas con datos personales de menores de edad, personas en estado de interdicción o incapacidad declarada por ley.

Menores de edad

1

Padres

1.-Documento que acredite la identidad de menor.

2.-Acta de nacimiento del menor.

3.-Identificación oficial del padre o de la madre, que pretenda ejercer el derecho.

4.-Carta en la que se manifieste, bajo protesta de decir verdad, que el padre o la madre es quien ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

2

Persona distinta a los padres

1.- Los documentos del punto 1 y 2 de la primera columna.

2.-Documento legal que acredite la posesión de la patria potestad.

3.-Identificación oficial de quien presenta la solicitud y posee la patria potestad.

4.-Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

3

Tutor

- 1.- Los documentos del punto 1 y 2 de la primera columna

2.-Documento legal que acredite la tutela.

3.-Identificación oficial del tutor.

4.-Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la tutela.

Personas en estado de interdicción o incapacidad legal

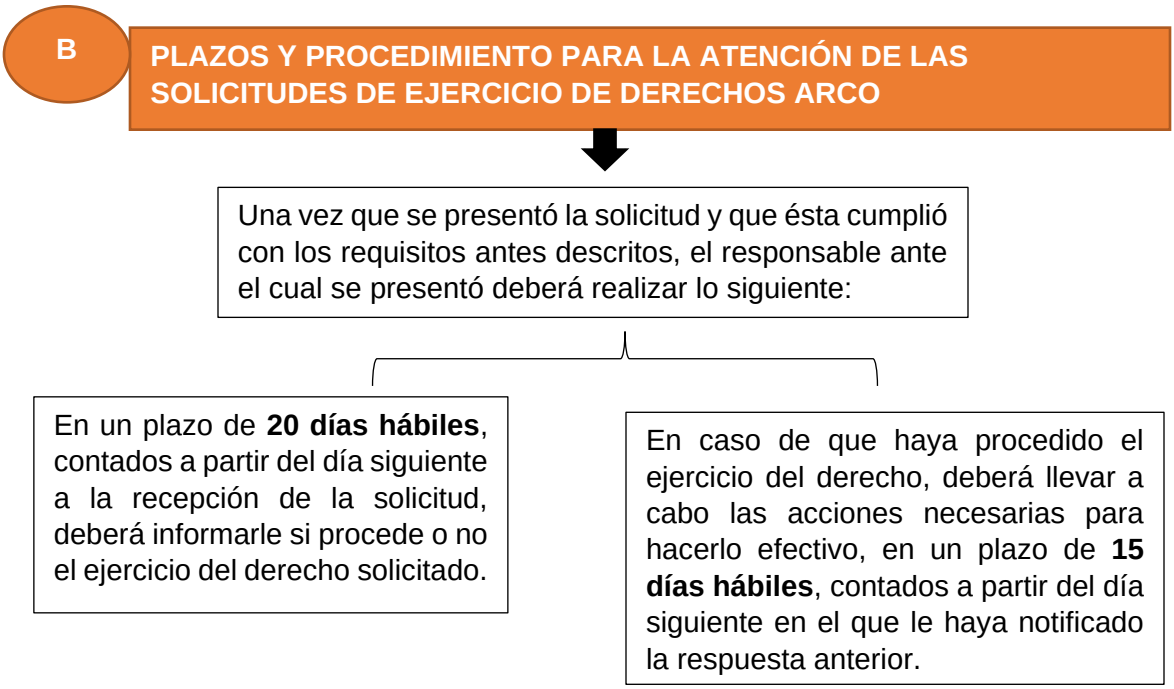
- Documento que acredite la identidad del titular de los datos personales.
- Instrumento legal de designación del tutor.
- Identificación oficial del tutor.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de lo alguno de los supuestos legales de suspensión o limitación de la misma.

Personas fallecidas

- Identificación de la persona a quien pertenecían los datos personales.
- Acta de defunción correspondiente.
- Documento(s) que acrediten el interés jurídico de quien presenta la solicitud; aquél donde el titular de los datos personales hubiere expresado fehacientemente su voluntad de que esta persona ejerza los derechos ARCO con relación a sus datos personales, o el mandato judicial que en su caso exista para dicho efecto.
- Documento de identificación oficial de quien presenta la solicitud.

Se entenderá por interés jurídico aquel derecho subjetivo derivado de una ley que permite a una persona actuar a nombre de otra que por su situación le es imposible. Ello, a efecto de solicitar el ejercicio efectivo de los derechos ARCO.

Quienes pueden alegarlo son, de manera enunciativa más no limitativa: el albacea, los herederos, los legatarios o cualquier persona que haya sido designada previamente por el titular para ejercer los derechos ARCO en su nombre, lo cual se acreditará con copia simple del documento delegatorio, pasado ante la fe de notario público o suscrito ante dos testigos.



- Los plazos antes señalados se pueden ampliar por un periodo igual, cuando esté justificado y se le informe de ello. En caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo, en un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior.
- El ejercicio de los derechos ARCO será sencillo y **GRATUITO**, sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación de documentos o envío de información.
- Por último, si la normatividad aplicable al tratamiento de datos personales en cuestión, establece un trámite o procedimiento específico para el ejercicio de los derechos ARCO, el sujeto obligado le deberá informar la existencia de dicho trámite o procedimiento en un plazo máximo de 5 días hábiles, contados a partir del día siguiente de la presentación de la solicitud, a fin de que usted decida si presentará su solicitud de acuerdo con el trámite específico o con base en el procedimiento aquí descrito.

Fuente: elaboración propia con los requisitos proporcionados en la página web del INAI. https://home.inai.org.mx/?page_id=3374

En el caso de que cualquier sujeto obligado no haga caso a alguna solicitud de derechos ARCO, el titular puede ejercitar algún procedimiento de impugnación en materia de

protección de datos personales ante el INAI, el cual proporciona el formato de solicitud a través de la siguiente liga electrónica: https://home.inai.org.mx/?page_id=3395

Así mismo, durante el análisis de la LGPDPPSO, reparé que existen algunos puntos que se pueden mejorar para la protección de datos personales en posesión de sujetos obligados, y son los siguientes:

- Desde el punto de vista de la suscrita, el artículo 14 en su fracción VIII establece que el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales promoverá "*la homologación y desarrollo de los procedimientos previstos en la presente Ley*"[223], para lo cual, considero los y las legisladores deben iniciar con un estudio para determinar qué tan factible es homologar la presente Ley, con la ley que regula a los particulares. Porque de manera esencial, estas dos leyes se encargan de proteger los datos personales. Así mismo, es importante determinar si es necesario exceptuar a las Sociedades de Información Crediticia, pues como se explicaba anteriormente, este es una persona jurídico colectivo que al final del día trata datos personales, y no tendría por qué quedar exenta de su regulación en la LFPDPPP.

  Este es un tema que incluso algunos panelistas expusieron durante la Jornada de difusión y reflexión: los alcances y desafíos de las leyes de protección de datos personales en posesión de particulares y sujetos obligados[224] hecha en junio de 2022 en que se proponía al legislador el estudio para homologar las obligaciones, derechos y responsabilidades de lo público y lo privado.

- En cuanto a la promoción e implementación de acciones para garantizar condiciones de accesibilidad para que los grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales, deben

[223] Artículo 14 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 2 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

[224] Jornada de difusión y reflexión: los alcances y desafíos de las leyes de protección de datos personales en posesión de particulares y sujetos obligados. INAI. Trasmitido en YouTube. Consultado el 17 de abril de 2023. Disponible en: https://www.youtube.com/watch?v=D-gMoTHF9JU&t=12699s

de existir mayores esfuerzos para lograr ese objetivo, pues en el estudio “Los jóvenes y la ciberseguridad en zonas rurales del estado de Oaxaca. Caso: Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO), plantel 165”[225] realizado por Norma Martínez López y Roselia Martínez López, al menos el 42.9% de los encuestados en dicho plantel no saben cómo protegerse ante cualquier tipo de amenaza en internet. Además, el 56.3% de los jóvenes encuestados dicen no conocer las medidas básicas de la seguridad de la información; y pesar de que el 92.9% de los encuestados dicen conocer que tienen derecho a la intimidad de sus datos personales y que el 98.2% de ellos mencionan que saben que son los derechos ARCO. Con estos datos de un pequeño grupo de la población en situación de vulnerabilidad, queda sobreentendido que se requiere un mayor esfuerzo tanto por las instituciones de gobierno y los particulares para difundir los procedimientos de protección de datos personales en los grupos vulnerables.

En este orden de ideas, el artículo 93 de la Ley establece que el Instituto y Organismos garantes deberán promover *“que en los programas y planes de estudio, libros y materiales que se utilicen en las instituciones educativas de todos los niveles y modalidades del Estado, se incluyan contenidos sobre el derecho a la protección de datos personales, así como una cultura sobre el ejercicio y respeto de éste;*”[226], sin embargo, partiendo del mismo estudio de Norma y Roselia Martínez, sólo el 32.1% del total de los jóvenes encuestados saben sobre la existencia de la Ley Protección de Datos Personales de su país y el 81.3% de ellos no conocen las instituciones enfocadas de proteger los datos personales.

[225] Martínez López, Norma; Martínez López, Roselia. Los jóvenes y la ciberseguridad en zonas rurales del estado de Oaxaca. Caso: Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO), plantel 165. RECAI Revista de Estudios en Contaduría, Administración e Infomática, vol. 7, núm. 20, 2018. Universidad Autónoma del Estado de México, México. Consultado el: 27 de abril de 2023. Disponible en: https://www.redalyc.org/articulo.oa?id=637968308002

[226] Artículo 93 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 2 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Así mismo, este mismo artículo en su fracción II estipula que el Instituto y los Organismos garantes impulsarán "*en conjunto con instituciones de educación superior, la integración de centros de investigación, difusión y docencia sobre el derecho a la protección de datos personales que promuevan el conocimiento sobre este tema y coadyuven con el Instituto y los Organismos garantes en sus tareas sustantivas*"[227], empero, casi ningún instituto de educación superior en México, cuenta con un centro de investigación especializado en materia de protección de datos personales.

- La LGPDPPSO que fue publicada en el 2017, contempla la protección de datos personales desde una perspectiva más amplia y hace alusión a no ser objeto de decisiones automatizadas, redactándolo en el artículo 47 fracción II de la siguiente manera "*El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando: […] Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento*."[228], empero, demostró a lo largo de este trabajo de investigación que el gobierno y los particulares hacen tratamientos automatizados sin intervención humana para obtener algún tipo de ventaja o beneficio para sí mismos, en muchos casos de este tratamiento automatizado, los titulares no saben que sus datos personales se están usando para algún fin en específico que ellos no conocen.

[227] *Idem*.
[228] Artículo 47 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 2 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

En este sentido, se requiere mayor esfuerzo por parte de gobierno, instituciones y empresas para difundir en la población una cultura de protección de datos personales, así como hacer del conocimiento de las personas quiénes, y a través de qué mecanismos que ejercen los derechos ARCO y en general, los derechos de protección de datos personales y de privacidad.

- Por otra parte, existe una contradicción en cuanto el artículo 74 y 79 de la Ley. El primero estipula:

> "Artículo 74. *Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto o los Organismos garantes, según corresponda, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales*."[229]

Ahora bien, el artículo 79 menciona:

> "*Artículo 79. Cuando a juicio del sujeto obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la Evaluación de impacto en la protección de datos personales."*[230]

[229] Artículo 74 y 79 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 2 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
[230] *Idem*.

Estos dos artículos presentan una laguna legal; primero porque el artículo 74 de la Ley permite en cierto modo a el responsable modificar sus políticas públicas, sus plataformas digitales, aplicaciones o cualquier otro tipo de tecnología que trate datos personales, a pesar de hacer una evaluación de impacto, y luego presentarla al INAI o a cualquier de los organismo garantes (aunque estos no emitan una recomendación vinculante y ejecutable en caso de que dicho cambio en la política pública o en los sistemas informáticos traten de manera ilegal o eviten cumplir con estándares mínimo de protección de datos personales) y después el artículo 79 estipula que cuando afecte a los intereses del responsable realizar una evaluación de impacto, esta no será necesario llevarse a cabo. En opinión de la suscrita, este artículo debe ser reformando y darle la potestad al INAI para que pueda exigir la realización de la evaluación de impacto cuando exista una adecuación a políticas públicas o sistemas informáticos. También para que el Instituto pueda emitir criterios vinculantes en dado caso de que dicha adecuación políticas públicas o sistemas informáticos no garantice la protección de datos personales.

- Existe un capítulo que requiere mucha atención y análisis para saber de qué manera se cumplen sus normas. El capítulo referente a las Bases de Datos en Posesión de Instancias de Seguridad Pública, Procuración y Administración de Justicia, regula a estas entidades para determinar cómo tienen que tratar los datos personales, sin embargo, presenta dudas en cuanto al cumplimiento verdadero. Durante el capítulo II del presente trabajo de investigación se demostró que existen instituciones que tratan los datos personales de las personas sin su consentimiento y poniéndolas en un escenario de desventaja, al “marcarlas” en sus bases de datos como “peligrosas” o “potencialmente peligrosas” (caso de la GN).

  La Seguridad Nacional y ciberseguridad es todavía un tema con muchas aristas para reflexionar y entender cómo la tecnología y la inteligencia artificial deben

usarse adecuadamente para tratar datos personales de las personas, sin que exista una afectación directa a su persona y vida privada. A juicio de la suscrita, de los principales elementos para evitar que cualquier ente o persona haga uso indebido de nuestros datos personales es establecer lineamientos que aseguren un correcto uso de estas tecnologías y fomentar en la sociedad una cultura de cuidado y protección de los datos personales.

4.4 Marco jurídico del derecho a la privacidad en México

En México no existe ninguna ley que explícitamente regule de manera particular el derecho a la privacidad, sin embargo, este derecho es ejercible de manera indirecta por otras leyes, como la Ley Federal de Protección de Datos Personales en Posesión de Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, además de otros mecanismos internacionales entre ellos la Declaración Universal de los Derechos Humanos en su artículo 12 y el Pacto Internacional de Derechos Civiles y Políticos con su artículo 17. Por su parte la ONU, a través del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) emitió en el septiembre de 2019 su resolución A/HRC/RES/42/15 sobre el derecho a la privacidad en la era digital, sin embargo, esta resolución no es vinculatoria y representa una mera recomendación.

Desde 2013, la Asamblea General de las Naciones Unidas y el Consejo de Derechos Humanos han aprobado numerosas resoluciones sobre el derecho a la privacidad en la era digital[231]. En cuanto a la resolución de la ACNUDH, se emiten una serie de recomendaciones a los Estados y las empresas para garantizar el derecho a la privacidad y la protección de los datos personales muy específicamente en la era digital.

[231] ACNUDH. Normas internacionales relativas a la privacidad digital. El ACNUDH y la privacidad en la era digital. Consultado el 02 de mayo de 2023. Disponible en: https://www.ohchr.org/es/privacy-in-the-digital-age/international-standards-relating-digital-privacy#:~:text=El%20art%C3%ADculo%2012%20de%20la,a%20su%20honra%20y%20reputaci%C3%B3n

a) La autorregulación

A pesar de que no existen leyes específicas que protejan la privacidad digital, hay otras formas de convertirla exigible, como lo es la Autorregulación. La Autorregulación se promueve en la LFPDPPP, en su artículo 44 en la cual estipula lo siguiente:

> *"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."*[232]

Si bien no se estipula directamente una protección a la privacidad digital, si se estipula una autorregulación a la protección de los datos personales, los cuales, son elemento clave e importante para garantizar la privacidad en la era digital. De acuerdo con Carmen Quijano "la autorregulación es una buena alternativa ya que son las empresas privadas las que cuentan con la experiencia, capacidad y recursos necesarios para hacer frente a los retos del ciberespacio, además, se evita la necesidad de seguir un proceso legislativo formal, que puede ser complejo y tardado"[233]. Si bien la autorregulación representa una

[232] Artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Consultado el 2 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[233] Quijano Decanini, Carmen.2022. Derecho a la privacidad en internet. Tirant lo blanch. México. Pág. 216.

excelente oportunidad para que el derecho vaya de la mano con los avances tecnológicos, también este esquema de autorregulación requiere de profesionales comprometidos con cumplir los principios y estándares de protección de datos personales y de privacidad. Requiere además que las empresas o los Estados garanticen la transparencia y rendición de cuentas, así como la participación de la sociedad en general, para generar conciencia sobre la importancia que tiene cuidar nuestra privacidad y datos personales en una era hiperconectada a las nuevas tecnologías.

Dado el contexto anterior, se propone el esquema de co-autorregulación, en donde las empresas/Estado se adhiera a los principios básicos de protección de datos personales y del derecho a la privacidad en la era digital, así como las normas sancionadoras y coercitivas que el Estado les pueda imponer a aquellos responsables del mal tratamiento de datos personales. En el caso de México, el reglamento de la LFPDPPP estipula, por ejemplo, en su principio de responsabilidad que aquellos responsables del tratamiento de datos personales con un esquema de autorregulación también tienen la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia y posesión (artículo 47), pero ni en la Ley ni el Reglamento se estipula que en cuanto a un incumplimiento de los principios jurídicos y estándares de protección de datos y privacidad los responsables que eligen este esquema se van a someter a la jurisdicción y sanciones del Estado,

La autorregulación y co-autorregulación son una excelente forma de adecuar de forma rápida las normas de protección de datos y privacidad, pero puede parecer como una especie de disfraz para simular con el cumplimiento de las normas, y más bien puede representar los intereses particulares de las empresas, Estados o cualquier persona en general que trate datos personales. Al respecto, Ernesto Villanueva argumenta que “los sistemas de autorregulación por sí solos no han dado los resultados que la sociedad requiere porque descansan en la libre voluntad de los sujetos involucrados. Tampoco, sin embargo, la regulación ha podido encargarse de resolver este reto, … pero parece

haber un consenso de que internet no puede ser una zona de excepción o impunidad normativa"[234].

b) Mecanismos jurisdiccionales nacionales

Desafortunadamente en México no hay ninguna ley que de manera expresa y directa proteja el derecho a la privacidad, pero como se mencionó anteriormente, este derecho es ejercible a través de otros mecanismos jurídicos. Encontramos en primer término en que en las leyes de protección de datos, estos de alguna forma tratan de proteger el derecho a la privacidad en la era digital porque establecen lineamientos para que los particulares o el Estado usen de manera muy limitada los datos personales; así como el que lleven una recopilación de datos de forma legal; que los mantengan actualizados; que no intente crear algún tipo de mecanismos artificial que logre identificar al posible titular de los datos; entre otros supuestos. Pero como también se analizó anteriormente, estas leyes referentes a la protección de datos carecen de eficacia y modernidad, ya que la Ley Federal de Protección de Datos Personales en Posesión de Particulares tiene más de 12 años (hasta esta fecha en que la suscrita realiza este trabajo de investigación) sin ser actualizada y adecuada a las nuevas exigencias del mercado global, digitalizado e innovador. Al respecto, diversas figuras públicas entre las que se encuentran algunos y algunas Comisionadas del INAI, legisladoras, legisladores; así como docentes, doctrinarios, doctrinarias y conocedores del tema coinciden con que las actuales leyes deben volverse a estudiar y mejorar. Sobre todo, la LFPDPPP que necesita ser adecuada a la realidad actual para evitar una intromisión sin consentimiento a la vida privada de las personas.

c) El Juicio de Amparo

El Amparo protege de manera indirecta el derecho a la privacidad a través de los derechos ARCO, esto debido a que la LGPDPPSO estipula que en caso de que las resoluciones de los Organismos garantes no favorezcan a los intereses del titular de los

[234] Cit. por Quijano Decanini, Carmen.2022. Derecho a la privacidad en internet. Tirant lo blanch. México. Pág. 216.

datos personales y esto conlleve una violación a sus derechos ARCO o derechos humanos, estos pueden acudir ante el Instituto o la Suprema Corte de Justicia de la Nación (SCJN). Cuando el titular no reciba acuerdo favorable al haber promovido un recurso de revisión ante el Instituto, o ante los Organismos garantes, o la Unidad de Transparencia del responsable que haya conocido de la solicitud para el ejercicio de los derechos ARCO, la LGPDPPSO faculta al titular para que interponga un Amparo. La Ley lo estipula en su artículo 115 de la siguiente manera:

> "Artículo 115. […]
>
> *Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación mediante el Juicio de Amparo*"[235].

Por su parte el artículo 116 menciona que:

> "Artículo 116. *Tratándose de las resoluciones a los recursos de revisión de los Organismos garantes de las Entidades Federativas, los particulares podrán optar por acudir ante el Instituto interponiendo el recurso de inconformidad previsto en esta Ley o ante el Poder Judicial de la Federación mediante el Juicio de Amparo."*[236]

Ahora bien, cuando los titulares crean que las resoluciones de los recursos de inconformidad interpuestos ante el Instituto vulneran sus derechos ARCO y su derecho a la privacidad, pueden interponer Amparo de acuerdo con el artículo 129:

> "Artículo 129. […]
>
> *Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación mediante el Juicio de Amparo."*[237]

[235] Artículo 115 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 2 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
[236] Artículo 116 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 2 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
[237] Artículo 129 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultado el 2 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Es importante aclarar que para ejercer nuestros derechos a la protección de datos personales y el derecho a la privacidad a través de la figura del Amparo solo se puede promover cuando la figura del responsable corresponde a un Sujeto Obligado que regula la LGPDPPSO, y no tratándose de particulares. Por ello, la suscrita alienta al legislador y legisladora revisar de manera urgente la LFPDPPP para permitir que cualquier particular pueda interponer un Juicio de Amparo en situaciones de vulneración a los derechos ARCO y el derecho a la privacidad en la era digital. Así mismo, se recuerda que esta LFPDPPP debe de contemplar ahora a las Sociedades de Información Crediticia.

Para finalizar, no está de más mencionar que los responsables del tratamiento de datos personales tienen que otras medidas de protección de los derechos ARCO y del derecho a la privacidad, estas medidas pueden incluir el establecer medios alternativos de solución de controversias (MASC) para logar que la protección al titular de los datos sea rápida, eficiente y expedita. Así pues, con estos MASC se logra llegar a una rápida solución ante un futuro problema, beneficiando no sólo al titular de los datos sino también a las responsables del tratamiento, pues con ello ahorran tiempo, así como recursos humanos y monetarios.

4.5 Precedentes de la suprema corte de justicia de la nación (SCJN) que salvaguardan el derecho de protección de datos personales y el derecho a la privacidad en la era digital

A lo largo de todo este trabajo de investigación se demostró que el papel de las nuevas tecnologías, el internet y la inteligencia artificial en la vida de las personas se hace cada día indispensable. Esto se debe en parte a los grandes beneficios que estas herramientas tecnológicas aportan en la vida de las personas, pero también se comprobó que existen situaciones en las que el uso desmedido y sin seguridad de estas herramientas tecnológicas pueden representar una amenaza para la sociedad.

El fenómeno de la globalización ha permitido que la economía mexicana avance, y con ello se permitió la entrada al país de empresas tecnológicas extranjeras, lo cual, permitió a México experimentar junto con otros países en el uso de las tecnologías de la

información, la inteligencia artificial, el internet, la neuro tecnología, el internet de las cosas entre otros; pero fue justo con la llegada de estas herramientas que México está comprobando que la legislación actual necesita ser adecuada a la realidad tecnológica que se vive día con día.

El máximo tribunal del país tuvo acceso a algunos casos que involucraron realizar un ejercicio de ponderación de los derechos digitales de las personas y de los intereses particulares de las empresas (nacionales o extranjeras) o el gobierno. Entre algunos de los precedentes más actuales que emitió la SCJN sobre el derecho a la protección de datos personas y el respeto a la privacidad en la era digital figuran los siguientes:

> **DATOS PERSONALES. LA LICENCIA DE USO DE UN SIGNO MARCARIO RELATIVO A LA PRESTACIÓN DEL SERVICIO DE MOTOR DE BÚSQUEDA EN INTERNET CONCEDIDA POR UNA EMPRESA EXTRANJERA EN FAVOR DE UNA SOCIEDAD MERCANTIL MEXICANA, ES APTA PARA CONSIDERAR LA RESPONSABILIDAD DE ÉSTA POR EL TRATAMIENTO DE AQUÉLLOS CONFORME A LA NORMATIVA CONSTITUCIONAL Y LEGAL RESPECTIVA.**
>
> De acuerdo con los artículos 87, 88, 125, 126, 136, 139, 140 y 141 de la Ley de la Propiedad Industrial, el titular de una marca puede conceder una licencia de uso a favor de un tercero, quien quedará obligado a vender los productos o prestar los servicios de que se trate, con la misma calidad que los comercializados por el titular, ejercer las acciones legales de protección de los derechos y usar la marca como si fuera el propietario del registro. Así, la licencia de uso de un signo marcario relativo a la prestación del servicio de motor de búsqueda en Internet concedida por una empresa extranjera en favor de una sociedad mercantil constituida en términos de los artículos 3o., 4o., 6 bis y 15 del Código de Comercio y 1o., fracción III, 4o., 5o., 58, 59 y 73 de la Ley General de Sociedades Mercantiles, es apta para considerar la responsabilidad de ésta por el tratamiento de datos personales de un gobernado, en tanto que su constitución en territorio nacional, en adición a la licencia concedida en su favor, la legitiman y obligan a prestar ese servicio en México y, por tanto, a responder

> por su actuación conforme a la Constitución Federal y a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[238].

Este precedente nos explica que ahora las empresas que se constituyan con la normatividad mexicana, pero usando la licencia de uso de un signo marcario de un motor de búsqueda adquiere cualquier tipo de responsabilidad ante la sociedad mexicana a la cual le brinda el servicio. Esta tesis aislada surgió del caso Pablo Agustín Meouchi Saade vs. Google México, en la cual Pablo Agustín Meouchi Saade solicitó a Google México, S. de R. L. de C. V. la cancelación de sus datos personales respecto de la información que aparece en el navegador denominado "Google" y "YouTube"[239].

Por otra parte, la Jurisprudencia con registro digital 2026242 argumenta que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales permite que el instituto puede emitir normas generales tanto sustantivas como adjetivas en materia de derecho sancionador, esto porque el INAI debe de contar con los mecanismos necesarios para el cumplimiento de sus deberes constitucionales. Dicha jurisprudencia es la siguiente:

> **INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES. DADO SU CARÁCTER DE ÓRGANO CONSTITUCIONAL AUTÓNOMO, CUENTA CON ATRIBUCIONES PARA EMITIR NORMAS GENERALES TANTO SUSTANTIVAS COMO ADJETIVAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES, INCLUIDAS AQUELLAS EN MATERIA DE DERECHO ADMINISTRATIVO SANCIONADOR.**
>
> […] Criterio jurídico: La Segunda Sala de la Suprema Corte de Justicia de la Nación determina que la competencia constitucional otorgada al INAI para conocer de la materia de protección de datos personales en posesión de los particulares le concede amplias atribuciones, entre las que se encuentran la facultad de emitir normas generales tanto sustantivas como adjetivas en

[238] Tesis: I.10o.A.120 A (10a.), Gaceta del Semanario Judicial de la Federación. Libro 70, septiembre de 2019, Tomo III, página 1853.
[239] AMPARO DIRECTO EN REVISIÓN 3800/2019. RECURRENTES: GOOGLE MÉXICO, SOCIEDAD DE RESPONSABILIDAD LIMITADA DE CAPITAL VARIABLE Y GOOGLE INC. QUEJOSO: PABLO AGUSTÍN MEOUCHI SAADE. Consultado el 23 de mayo de 2023.

materia de protección de datos personales, ello en la medida de que, en su carácter de órgano constitucional autónomo, debe contar con las herramientas necesarias para el cumplimiento de sus deberes constitucionales. Bajo esa óptica, tanto los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones, emitidos por el INAI para instaurar procedimientos sancionatorios, como la demás normativa que emita, incluida aquella en materia de derecho administrativo sancionador, serán acordes con el orden constitucional, siempre que tengan la finalidad de que el órgano constitucional autónomo cumpla con sus funciones y no se contravengan abiertamente disposiciones legales.

Justificación: El artículo 6, apartado A, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos, dispone que la Federación contará con un organismo autónomo especializado, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y la protección de datos personales en posesión de sujetos obligados, el cual se regirá conforme a las bases que dispongan las leyes en esa materia que emita el Congreso de la Unión. Para cumplir con el deber encomendado debe realizar diversos procedimientos, entre los cuales están aquellos que tienen como finalidad sancionar a los infractores. En ese sentido, las bases de los procedimientos de investigación y de los sancionadores están previstas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y, por ello, el INAI cuenta con atribuciones para emitir normas que los detallen, siempre que tengan una vinculación directa e inmediata con la debida observancia del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados[240].

Así mismo, la SCJN estableció en dos tesis que México debe de crear los mecanismos legales suficientes para que su población esté protegida ante cualquier riesgo que presentan las herramientas tecnológicas, que a la letra argumentan:

PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE

[240] Tesis: 2a./J. 17/2023 (11a.). Gaceta del Semanario Judicial de la Federación. Libro 23, marzo de 2023, Tomo III, página 2236

POTENCIALIZARSE ANTE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS.

Conforme al proceso legislativo de la adición del segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicada el 1 de junio de 2009 en el Diario Oficial de la Federación, en relación con la interpretación del artículo 11, numeral 2, de la Convención Americana sobre Derechos Humanos, efectuada en diversos criterios emitidos por la Corte Interamericana de Derechos Humanos, el deber del Estado frente al derecho de los gobernados a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de los individuos que integran la sociedad, y que conlleva la obligación de dejarlos exentos e inmunes a invasiones agresivas o arbitrarias por parte de terceros o de la autoridad pública, debe potencializarse ante las nuevas herramientas tecnológicas. Lo anterior, por el efecto multiplicador de los medios de comunicación digitales de Internet y las redes sociales, a través de los cuales se facilita la difusión y durabilidad de su contenido, al permanecer de manera indefinida en los medios electrónicos en los que se publican, sin restricción territorial alguna; constituyéndose así en una constante invasión positiva o negativa, según el caso, a los derechos inherentes al ser humano, vinculados con el mencionado, como son la intimidad, el honor, la reputación, la vida privada y, consecuentemente, la dignidad humana[241].

PROTECCIÓN DE DATOS PERSONALES. CONSTITUYE UN DERECHO VINCULADO CON LA SALVAGUARDA DE OTROS DERECHOS FUNDAMENTALES INHERENTES AL SER HUMANO.

El párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce los denominados derechos ARCO, relativos al acceso, rectificación, cancelación y oposición de datos personales, como un medio para garantizar el derecho de los individuos a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de la sociedad, y la

[241] Tesis: I.10o.A.6 CS (10a.) Gaceta del Semanario Judicial de la Federación. Libro 70, septiembre de 2019, Tomo III, página 2200

> posibilidad de exigir su cumplimiento a las autoridades y particulares que conocen, usan o difunden dicha información. Así, dichas prerrogativas constituyen el derecho a la protección de los datos personales, como un medio de salvaguarda de otros derechos fundamentales previstos en la propia Constitución y en los tratados internacionales de los que México es Parte, conforme a los cuales, el Estado tiene la obligación de garantizar y proteger el derecho de todo individuo a no ser interferido o molestado por terceros o por una autoridad, en ningún aspecto de su persona –vida privada–, entre los que se encuentra el relativo a la forma en que se ve a sí mismo y cómo se proyecta a los demás –honor–, así como de aquellos que corresponden a los extremos más personales de la vida y del entorno familiar –intimidad–, o que permiten el desarrollo integral de su personalidad como ser humano –dignidad humana–[242].

En cuanto a la materia de competencia jurisdiccional para conocer de los asuntos en materia de protección de datos personales y vida privada que involucren a nacionales mexicanos y empresas extranjeras, la SCJN determinó que debido a que la ejecución de tal acto que afecte a la vida de las personas puede ser en cualquier parte del mundo, el juez competente para conocer del amparo indirecto es el juez de distrito ante el cual se promueve la demanda. Con ello, se presenta un precedente muy importante para resolver asuntos en los cuales los titulares de los datos presenten alguna vulneración de sus derechos de protección de datos personales y vida privada en un mundo global y digital. La tesis es la siguiente:

> **COMPETENCIA POR TERRITORIO PARA CONOCER DEL JUICIO DE AMPARO INDIRECTO PROMOVIDO CONTRA LA EMISIÓN, PUBLICACIÓN Y DIFUSIÓN DE CONTENIDO AUDIOVISUAL POR MEDIO DE REDES SOCIALES COMO "YOUTUBE", "FACEBOOK" Y "TWITTER". SE SURTE EN FAVOR DEL JUEZ DE DISTRITO ANTE EL QUE SE PRESENTÓ LA DEMANDA, AL TENER DICHOS ACTOS EJECUCIÓN EN MÁS DE UN DISTRITO.**

[242] Tesis: I.10o.A.5 CS (10a.) Gaceta del Semanario Judicial de la Federación. Libro 70, septiembre de 2019, Tomo III, página 2199

[…] Este Tribunal Colegiado de Circuito determina que cuando se reclaman la emisión, publicación y difusión de contenido audiovisual por medio de redes sociales como "Youtube", "Facebook" y "Twitter", es competente por razón de territorio para conocer del juicio de amparo indirecto el Juez de Distrito ante el que se presente la demanda, al tener dichos actos ejecución en más de un Distrito.

Justificación: Lo anterior, porque el contenido multimedia publicado en redes sociales puede ser difundido y, a su vez, compartido por medio de plataformas digitales como "Facebook", "Youtube" y "Twitter", permitiendo su acceso universal, es decir, cualquier persona con acceso a Internet y en cualquier demarcación geográfica podrá estar en aptitud de acceder a ese contenido (fotografías, videograbaciones, audios, entre otros), inclusive, compartirlo conforme a las políticas de cada red social. Asimismo, un programa de televisión (creado en un determinado Estado) y que también es publicado en dichas redes sociales –específicamente en las cuentas oficiales de las autoridades de las que se reclaman los actos– puede compartirse, en primer lugar, con la finalidad de darle publicidad a la información que se difunde y que sus usuarios tengan acceso a ella, sin importar el lugar en el que se encuentren y, en segundo, al tratarse de información o contenido (que el quejoso tiene interés en que no sea publicado, al ser figura pública) difundido en cuentas oficiales del gobierno del Estado, o bien, de figuras públicas en su gestión gubernamental, adquiere notoriedad pública y se convierte en relevante para el interés general, el cual no está limitado a una demarcación geográfica en específico, sino que su límite territorial se encuentra en que una persona tenga acceso a Internet en el lugar en el cual se encuentre. Por tanto, la ejecución de los actos reclamados se puede llevar a cabo en un Distrito distinto al Estado de Campeche, con independencia de que todas las autoridades responsables tengan su residencia en ese lugar pues, en el caso, la competencia se surte en razón de la naturaleza de la ejecución de los actos reclamados, no así del lugar de residencia de las autoridades responsables; en consecuencia, es competente para conocer y resolver de la demanda de amparo indirecto el Juez de Distrito ante quien se presentó, en términos de la fracción VII del artículo

> 107 de la Constitución Política de los Estados Unidos Mexicanos, en relación con el precepto 37, párrafo segundo, de la Ley de Amparo[243].

En México existe un caso parecido al anterior, conocido como Ulrich Richter Morales vs Google México. El afectado pidió a Google México suprimir la información que dañaban su imagen y su honor. Pero Google México argumentó que no tenía competencia para poder suprimir datos de plataformas que pertenecen a Google Inc. Luego de varias remisiones a otros juzgados, fue así como el asunto llegó a la SCJN y presentaba una gran oportunidad para México establecer un precedente que estableciera la competencia legal de los jueces mexicanos para resolver asuntos en los que involucren a su población y a empresas multinacionales que argumenten regirse por las leyes de sus países de origen. Desafortunadamente el 6 diciembre de 2017 Google Inc. Se desiste del recurso de revisión que interpuso ante la SCJN. Sin embargo, la citada empresa multinacional, por conducto de su apoderado legal, desistió del recurso de revisión y, con ello, ya no resultó posible hacer pronunciamiento alguno sobre el fondo de la decisión adoptada por el juez de distrito.

Por todo ello, la Primera Sala resolvió tener a la parte quejosa por desistida, dejar firme la sentencia recurrida y declarar sin materia la revisión adhesiva[244].

Por otro lado, es plausible que México comience a proteger el derecho de protección de datos de personas fallecidas[245] así como prevenir la violencia digital juzgando con una perspectiva de género[246]. Si bien los jueces en México comienzan a analizar asuntos relacionados a los derechos digitales de sus ciudadanos, esta materia necesita seguir estudiándose, sobre todo porque aún faltan diversos tópicos que regular, todos relacionados con el uso y tratamiento de datos personales y la era digital, la inteligencia artificial, las neuro tecnologías, entre otras.

---

[243] Tesis: XXX.3o.4 K (11a.). Gaceta del Semanario Judicial de la Federación. Libro 18, octubre de 2022, Tomo IV, página 3505

[244] Suprema Corte de Justicia de la Nación. Comunicados de Prensa. No. 194/2017. Consultado el 23 de mayo de 2023. Disponible en: https://www.internet2.scjn.gob.mx/red2/comunicados/noticia.asp?id=4639

[245] Consultar tesis 1a. V/2023 (11a.). Gaceta del Semanario Judicial de la Federación. Libro 23, marzo de 2023, Tomo II, página 2057

[246] Ver tesis I.3o.C.469 C (10a.). Semanario Judicial de la Federación.

4.6 La protección internacional del derecho a la privacidad y el derecho a la protección de datos personales

La protección internacional a los derechos ARCO y el derecho a la privacidad es más amplia, pues existen Declaraciones, Reglamentos y Recomendaciones de distintos países y de distintas organizaciones internacionales que se encargan de estudiar la parte jurídica de la era digital. Como resultado de esas investigaciones y análisis de la era digital y su repercusión a la vida de las personas, la ONU a través de las diversas Resoluciones que desde el 2013 emitió la Asamblea General de las Naciones Unidas y el Consejo de Derechos Humanos emitió numerosas recomendaciones a los Estados y las empresas para que protejan los datos personales y el derecho a la privacidad en la era digital, esto debido al rápido avance que las tecnologías e inteligencia artificial, los cuales si no se les presta la debida atención el impacto que tienen en la vida de las personas, puede tener un efecto muy grave, como limitar y vulnerar sus derechos fundamentales. En este sentido, México ratifico uno de los importantes Convenios en materia de protección de datos personales, y es el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, o mejor conocido como convenio 108 el cual garantiza el respeto de derechos y deberes de las personas físicas, derecho a la vida privada con respecto al tratamiento automatizado de sus datos de carácter personal, entre otras ventajas, como permitir el intercambio efectivo y seguro de la información, además de fortalecer las relaciones comerciales al establecer un flujo transfronterizo con reglas homogéneas entre los miembros[247].

Además de la correcta adopción del Convenio 108 como un instrumento jurídico y vinculante por parte de México, la suscrita considera que los legisladores del país deben adecuar las normas existentes, o en su caso, crear una Ley específica que trate la materia de la privacidad digital, y que abarque distintos aspectos y elementos que hoy en día presentar un riesgo a la vida privada de las personas.

[247] Infoem. 2021. Convenio 108 permite a México el intercambio efectivo y seguro de información. Consultado el 2 de mayo de 2023. Disponible en: https://www.infoem.org.mx/es/contenido/noticias/convenio-108-permite-m%C3%A9xico-el-intercambio-efectivo-y-seguro-de-informaci%C3%B3n

En cuanto a crear una ley específica que regule diversos tópicos que abarque el tema de protección de datos personales, el derecho a la privacidad, la regulación de la neurotecnología y la inteligencia artificial, México puede partir con lagunas recomendaciones que hace la Unión Europea y diversos de sus países. Por ejemplo, en el año 2021 España creó la Carta de los Derechos Digitales[248], el cual, emite una numerosa serie de recomendaciones muy útiles para legislar sobre la materia. Algunos de los temas que trata dicha Carta de los Derechos Digitales son:

- Derechos y libertades en el entorno digital.
- Derecho a la identidad en el entorno digital.
- Derecho a la ciberseguridad.
- Derecho a la herencia digital.
- Derecho a la igualdad y a la no discriminación en el entorno digital.
- Protección de las personas menores de edad en el entorno digital.
- Accesibilidad universal en el entorno digital.
- Derecho a la neutralidad de Internet.
- Derecho a recibir libremente información veraz.
- La empresa en el entorno digital.
- Derecho a un desarrollo tecnológico y un entorno digital sostenible.
- Derecho a la protección de la salud en el entorno digital.
- Libertad de creación y derecho de acceso a la cultura en el entorno digital.
- Derechos ante la inteligencia artificial.
- Derechos digitales en el empleo de las neuro tecnologías.

Esta Carta por los Derechos Digitales es una excelente base para adecuar las normas mexicanas que protegen el derecho a la vida privada y a los datos personales. O mejor aún, para que los y las legisladoras en México estudien a profundidad un tema tan importante como son los derechos digitales y logren mejorar dicha Carta por los Derechos Digitales. Además, dichas normas mexicanas deberían tener sí o sí un carácter

[248] Ver Carta de los Derechos Digitales de España. Disponible en: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

vinculante, así como que exijan el cumplimiento de la ley y la transparencia en las actuaciones de los responsables del tratamiento de datos.

CONCLUSIONES

En el capítulo I de este trabajo de investigación, se ofreció una delimitación conceptual de los elementos más importantes que se necesitan entender para la protección de datos personales, con ello, se pudo comprender cuál es la diferencia entre datos personales y datos personales sensibles, así como entender cómo las normas mexicanas los regulan. Al mismo tiempo, se ofreció un panorama general sobre el alcance del derecho a la imagen, el derecho al honor, el derecho a la intimidad, y el derecho a la privacidad, los cuales, todos ellos, sí como el derecho a la protección de datos personales pertenecen al derecho a la vida privada. Para salvaguardar todos estos derechos en un contexto digital, se requiere de mecanismos legales y herramientas que los particulares o sujetos obligados deben proporcionar a los titulares de los datos, es por eso por lo que surgen los derechos ARCO y los principios de protección de datos personales.

Sea que se traten los datos de manera física o digital, todos los responsables del tratamiento de datos tienen la obligación de proporcionar los famosos avisos de privacidad en los cuales se abarquen, como mínimo, los principios de protección de datos personales. De igual manera, está investigación en su capítulo I tuvo el propósito de recordar la importancia que tiene la autodeterminación informativa y la neutralidad de la red para que la sociedad pueda navegar en la red digital de manera libre, informada, autónoma y sin sufrir algún tipo de discriminación.

En el caso del capítulo II, este proporcionó un panorama actual del uso y tratamiento de los datos personales en la era digital. Se demostró que las empresas hacen de los datos de sus usuarios un elemento para incrementar sus ingresos, y que cuando se usan de manera ilegítima y desproporcional estas empresas adquieren un carácter de monopolio en el mercado digital y fomentan el consumismo sin consciencia.

En el caso del contexto político, los titulares de los datos presentan serios problemas al momento de poder ser manipulables por las mismas empresas que tratan sus datos personales y venden su información a los partidos políticos para ganar una elección. En Caso de Facebook y Cambrige Analytica nos recuerda que, en tiempo electores, nuestros datos pueden ser analizados por los políticos para manipular nuestro contexto

digital y nuestras emociones y así lograr su victoria, aunque no velen por el bienestar de la ciudadanía.

Por lo que se refiere al tema de la inteligencia artificial, se desarrollaron algunos ejemplos en los cuales sino se les presta la atención debida puede provocar duras consecuencias para la vida de las personas. Sea en el ámbito de la vigilancia masiva, del hackeo del internet de las cosas, en el uso de aplicaciones para clasificar y vender a las personas, etc.

Para el caso de los delitos cometidos en la red, estos son muy preocupantes porque más de la mitad de la población en México usa el internet y en muchas ocasiones no dimensiona el poder que tienen sus datos en ella. Además, se demostró que la mayoría de la población mexicana no sabe cómo proteger sus datos personales en la red digital. Y tampoco sabe a quién acudir cuando se le presenta un problema con sus datos personales. Por ello, se dedicó también un apartado que explicaba la importancia de la ciberseguridad en México, dado que los casos de ciberdelincuencia aumentan con el paso de los años en México y el mundo. También se vislumbró la importancia que tiene proteger las infraestructuras críticas de información, en las cuales, la mayoría de las personas, sino es que todas, requieren de su correcto funcionamiento para realizar sus actividades diarias.

Al final de este capítulo se consideró necesario ofrecer algunas recomendaciones para que la sociedad en general sepa cómo proteger sus datos personales en la red digital.

En cuanto al tercer capitulado, se proporcionó una explicación sobre el *Habeas Data*, como mecanismo jurídico usado en algunos otros países para proteger los datos personales, siendo la base de la inspiración para la creación de este instrumento jurídico la Declaración Universal de los Derechos Humanos y diversos tratados internacionales. Además de ser un recorrido por la historia del *Habeas Data*, se proporcionó una clasificación doctrinal de los distintos *Habeas Data* que existen para conocer las distintas formas en las que se puede ejercer el derecho de protección de datos personales.

Y finalmente en el capítulo IV se presentaron los mecanismos jurídicos para hacer efectivo el derecho de protección de datos personales y vida privada en una era digital

en México. También se analizaron diversos artículos de la Ley Federal de Protección de Datos Personales en Posesión de Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en los cuales se requieren muchas reformas y adecuaciones para definir mejor el alcance de ciertos principios, restricciones y atribuciones de los encargados del tratamiento de datos.

Una de las cosas que más llamó mi atención en este apartado, fue que la SCJN ya comenzó a resolver asuntos relacionados con la materia, y más interesante resulta el caso de Ulrich Richter Morales vs Google México y el caso de Pablo Agustín Meouchi Saade vs Google México. En de Ulrich Richter Morales hubiera sido un excelente precedente para resolver futuras controversias entre las empresas tecnológicas extranjeras. Sin embargo, durante la investigación de precedentes me di cuenta de que no existe regulación ni tesis, ni jurisprudencias que traten temas de regulación de los datos personales y la vida privada con la inteligencia artificial, las neuro tecnologías.

De ahí que los y las abogados, las personas encargadas de administrar justicia, así como los funcionarios y servidores públicos y sociedad en general conozcan y comprenda la importancia que tiene saber proteger sus datos personales. Y también que sepan cuáles son los mecanismos jurisdiccionales y ante quién interponerlos para hacer valer sus derechos digitales.

PROPUESTAS

Durante mi investigación comprendí que en los últimos años México comenzó a proteger los datos personales en posesión de particulares y sujetos obligados en un contexto digital. Sin embargo, el estudio de la materia sigue estando en sus inicios. Aún se requiere una legislación más adecuada a la realidad actual y digital. Y también una mejor comprensión de cómo los datos personales se pueden usar para afectar la vida de una persona y vulnerar sus derechos humanos.

Por ello, mis propuestas para este trabajo de investigación son la siguientes:

1.- La primera propuesta es definitivamente aumentar la difusión de la cultura en el cuidado de datos personales en toda la sociedad. Así como la difusión de los distintos mecanismos jurídicos para su protección, ya que como se estudió, hasta el 2022 existen 88.6 millones de personas mayores de 6 años que usan todos los días el internet, con lo cual, cualquier persona se puede dar una idea de los muchos asuntos que pudiesen surgir por la vulneración de los derechos humanos de las personas usuarias de las tecnologías de la información y el internet.

2.- Realizar semestral o anualmente (dependiendo de los recursos humanos de las entidades encargadas de proteger los datos personales, así como el de las asociaciones civiles de México) el seguimiento del avance de la educación digital del país. A partir de ello, hacer publicaciones en las que se explique cómo y de qué manera se ha avanzado en el conocimiento de la protección de datos personales en la sociedad mexicana, y de esos datos, mejorar las prácticas o la formación de los y las mexicanas en su formación digital.

3.- Adecuar urgentemente la normatividad mexicana en materia de protección de datos personales en México, principalmente sus Leyes de protección de datos personales en posesión de sujetos obligados y de particulares. Así como agregar los temas de:

- Portabilidad de derechos personales.
- Derechos ARCO para las personas fallecidas.
- Incluir en la ley que regula a las particulares, a las sociedades de información crediticia.

- Mejorar la redacción en cuanto al alcance del tratamiento de los datos personales en el tema de la Seguridad Nacional.
- Adecuar el concepto jurídico de consentimiento para el uso de los datos personales dado un escenario digital.
- Contemplar los alcances y límites de la transferencia internacional de datos dato que el flujo de los datos en la era digital es rápida y global.
- Exigir el uso estricto del aviso de privacidad ante cualquier particular o sujeto obligado, tenga sus actividades en el mundo físico o digital.

4.- Tomar de inspiración diversas normativas de otros países del mundo que tiene mayor protección de datos personales. Entre los que destaco a España, con su famosa Carta de los Derechos Digitales creada en 2021, en donde la suscrita rescata los siguientes puntos a tratar en la normatividad mexicana:

- Derechos y libertades en el entorno digital.
- Derecho a la identidad en el entorno digital.
- Derecho a la ciberseguridad.
- Derecho a la herencia digital.
- Derecho a la igualdad y a la no discriminación en el entorno digital.
- Protección de las personas menores de edad en el entorno digital.
- Accesibilidad universal en el entorno digital.
- Derecho a la neutralidad de Internet.
- Derecho a recibir libremente información veraz.
- La empresa en el entorno digital.
- Derecho a un desarrollo tecnológico y un entorno digital sostenible.
- Derecho a la protección de la salud en el entorno digital.
- Libertad de creación y derecho de acceso a la cultura en el entorno digital.
- Derechos ante la inteligencia artificial.
- Derechos digitales en el empleo de las neuro tecnologías.

Lo aquí redactado representan mis propuestas que logré discernir con base a toda la información que se recabó a la largo de este trabajo de investigación. Sin duda alguna,

el tema sobre la regulación de la era digital es amplio y extenso. Seguramente los temas que se intentarán regular en unos 5, 10 o más años serán completamente distintos. Aun así, es un buen comienzo que las leyes mexicanas regulen estos temas, y que las y los estudiosos del derecho, así como aquellos que lo ejercen todos los días, estudien a profundidad el tema de los derechos digitales.

BIBLIOGRAFÍA

LIBROS, ARTÍCULOS DE REVISTAS Y PUBLICACIONES EN LÍNEA

ACNUDH. Normas internacionales relativas a la privacidad digital. El ACNUDH. https://www.ohchr.org/es/privacy-in-the-digital-age/international-standards-relating-digital-privacy#:~:text=El%20art%C3%ADculo%2012%20de%20la,a%20su%20honra%20y%20reputaci%C3%B3n

Asociación de Internet MX. 18º Encuesta Estudio sobre los Hábitos de Personas Usuarias de Internet en México 2022. https://irp.cdn-website.com/81280eda/files/uploaded/18%C2%B0%20Estudio%20sobre%20los%20Habitos%20de%20Personas%20Usuarias%20de%20Internet%20en%20Mexico%202022%20%28Socios%29%20v2.pdf

Asociación de Internet MX. 2022. Estudio sobre ciberseguridad en empresas, personas usuarias de internet y padres de familia en México. Segunda edición. https://irp.cdn-website.com/81280eda/files/uploaded/Encuesta%20Ciberseguridad%202022%20pu%CC%81blica%2020230119.pdf

Banco Pichincha. ¿Qué hacen los hackers y qué tipos existen? https://www.pichincha.com/portal/blog/post/que-es-un-hacker

Barragán, A. 2022. El ejército mexicano ve a las feministas como enemigas del Estado. https://elpais.com/mexico/2022-10-23/el-ejercito-mexicano-ve-a-las-feministas-como-enemigas-del-estado.html

Bazán, V. 2005. El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. Estudios Constitucionales, 3(2),85-139. ISSN: 0718-0195. https://www.redalyc.org/articulo.oa?id=82030204

BBC News Mundo. 2022. Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México. https://www.bbc.com/mundo/noticias-america-latina-63167331

BBC news mundo. Quiénes son los uigures, la etnia que China está deteniendo en “campos de reeducación”. 2018. https://www.bbc.com/mundo/noticias-internacional-45368245

BBC News mundo. Uigures en China: los motivos por los que China detiene a los miembros de esta minoría musulmana. 2020. https://www.bbc.com/mundo/noticias-51531714

Blas, F. 2009. Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales. Revista Derecho del Estado, (23),37-66. ISSN: 0122-9893. https://www.redalyc.org/articulo.oa?id=337630233002

BUSINESS INSIDER MÉXICO Los delitos cibernéticos en México podrán ser tema de Seguridad Nacional en México. https://businessinsider.mx/delitos-ciberneticos-mexico-considerados-tema-seguridad-nacional_tecnologia/#:~:text=De%20acuerdo%20con%20la%20Condusef,y%20banca%20m%C3%B3vil%20cada%20hora.

Calderón, C. México “clientazo” de los ciberataques: crecen 42% amenazas por internet. El Financiero. https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/

Carta de Derechos Digitales. 2021. Plan de Recuperación, Transformación y Resiliencia. Gobierno de España. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Cellan-Jones, R. 2016. Elecciones en Estados Unidos: ¿fue Facebook la clave para el triunfo de Donald Trump? BBC NEWS MUNDO. https://www.bbc.com/mundo/noticias-internacional-37946548

Cobos Campos, A. 2013. El contenido del derecho a la intimidad. Cuestiones constitucionales, (29), 45-81. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-91932013000200003&lng=es&tlng=es.

Colón Ferruzola Gómez, E., & Cuenca Espinosa, H. A. 2014. Cómo responder a un Delito Informático. Revista Ciencia Unemi, 7(11),43-50. ISSN: 2528-7737. https://www.redalyc.org/articulo.oa?id=582663858004

Corvalán, J. 2018. Inteligencia artificial: retos, desafíos y oportunidades – Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia. ARTIGOS. Rev. Investig. Const. 5 (1). Enero-abril 2018. https://www.scielo.br/j/rinc/a/gCXJghPTyFXt9rfxH6Pw99C/?lang=es

Equipo ORCA. 2019. 3 casos reales de delitos informáticos en México. https://blog.orcagrc.com/casos-de-delitos-informaticos-en-mexico

Estrada Avilés, J. EL DERECHO A LA INTIMIDAD Y SU NECESARIA INCLUSION COMO GARANTIA INDIVIDUAL. http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf

Fernández, Y. 2021. Qué es la Dark Web, en que se diferencia de la Deep Web y cómo puedes navegar por ella. Xataka Basics. https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedes-navegar-ella

Flores Ávalos, E. Derecho a la imagen y responsabilidad civil. https://archivos.juridicas.unam.mx/www/bjv/libros/4/1943/21.pdf

Gendler, M. 2019. Neutralidad de la red y servicios over the top: una compleja relación en el ecosistema de telecomunicaciones. PAAKAT: revista de tecnología y sociedad, núm. 17, pp. 1-17. https://www.redalyc.org/journal/4990/499063348008/html/

Global Forum on Cyber Expertise. The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection. https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

Gómez-Córdoba, A, Arévalo-Leal, S, Bernal-Camargo, D, & Rosero de los Ríos, D. 2020. El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. Revista de Bioética y Derecho, (50), 271-294. Epub 23 de noviembre de 2020. http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300017&lng=es&tlng=es.

González, F. 2019. Big data, algoritmos y política: las ciencias sociales en la era de las redes digitales. Cinta de moebio, núm. 65, abril-septiembre, pp. 267-280. https://www.redalyc.org/journal/101/10160628010/

González, L. 2018. Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros. Revista Estudios Socio-jurídicos, vol. 21, núm. 1, pp.209-244. https://www.redalyc.org/journal/733/73357886009/html/

Hernández, J. 2012. La protección de datos personales en Internet y el habeas data. Corte IDH. ISSN: 1317-9306. https://www.corteidh.or.cr/tablas/r32012.pdf

IBM. ¿Qué es un ataque cibernético? https://www.ibm.com/mx-es/topics/cyber-attack

INFOEM. 2021. Convenio 108 permite a México el intercambio efectivo y seguro de información. https://www.infoem.org.mx/es/contenido/noticias/convenio-108-permite-m%C3%A9xico-el-intercambio-efectivo-y-seguro-de-informaci%C3%B3n

Informe anual del relator especial para la libertad de expresión. 1999. OEA. https://www.oas.org/es/cidh/expresion/docs/informes/anuales/Informe%20Anual%201999.pdf

Instituto de Transparencia e Información Pública de Jalisco. Consideraciones sobre el habeas data y su regulación en distintos ámbitos. https://www.itei.org.mx/v3/documentos/estudios/estudio_habeas_data_6abr10.pdf

Jiménez, W. G., & Meneses Quintana, O. 2017. DERECHO E INTERNET: INTRODUCCIÓN A UN CAMPO EMERGENTE PARA LA INVESTIGACIÓN Y PRÁCTICA JURÍDICAS. Prolegómenos. Derechos y Valores, XX (40),43-61. ISSN: 0121-182X. https://www.redalyc.org/articulo.oa?id=87652654004

Jornada de difusión y reflexión: los alcances y desafíos de las leyes de protección de datos personales en posesión de particulares y sujetos obligados. INAI. Trasmitido en YouTube. https://www.youtube.com/watch?v=D-gMoTHF9JU&t=12699s

Kruikemeier, S. 2014. How political candidates use Twitter and the impacto on votes. Computers in Human Behavior 43: 131-139.

Leal Moya, L. 2005. Seguridad humana: La responsabilidad de proteger. Boletín mexicano de derecho comparado, 38(114), 1117-1138. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332005000300005&lng=es&tlng=es.

Martínez Devia, A. 2019. “La inteligencia artificial, el Big Data y la era digital: ¿una amenaza para los datos personales?”, Revista La Propiedad Inmaterial no. 27, Universidad Externado de Colombia, enero-junio 2019, pp.5-23. DOI: https://doi.org/10.18601/16571959.n27.01

Martínez López, N. y Martínez López, R. 2018. Los jóvenes y la ciberseguridad en zonas rurales del estado de Oaxaca. Caso: Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO), plantel 165. RECAI Revista de Estudios en Contaduría, Administración e Informática, vol. 7, núm. 20, 2018. Universidad Autónoma del Estado de México, México. https://www.redalyc.org/articulo.oa?id=637968308002

Matilde-Espino, Y. y Valencia-Pérez, L. 2022. Análisis bibliométrico de la producción científica sobre México en temas de ciberseguridad (2015-2020). CIENCIA ergo-sum, Revista Científica Multidisciplinaria de Prospectiva. https://www.redalyc.org/journal/104/10472165009/10472165009.pdf

Mayer, J. 2011.Tracking the trackers: where everybody knows your username. CIS The Center for Internet and Society. https://cyberlaw.stanford.edu/blog/2011/10/tracking-trackers-where-everybody-knows-your-username#pii_leakage_footnote_1

Mendoza Enríquez, O. 2018. Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. IUS. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., vol. 12, núm. 41, jan-jun, 2018, pp. 267-291. https://www.redalyc.org/pdf/2932/293258387015.pdf

Meraz Espinoza, A. 2018. Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales. IUS. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., vol. 12, núm. 41, jan-jun, pp. 293-310. https://www.redalyc.org/pdf/2932/293258387016.pdf

Merino, L. Libertad de expresión y derecho al honor: colisión de dos derechos entre medios de comunicación. Instituto de Investigaciones Jurídicas de la UNAM. https://revistas-colaboracion.juridicas.unam.mx/index.php/decoin/article/viewFile/33236/30200

Microsoft. Protéjase de phishing. https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

Muñoz de Alba Medrano, M. Habeas Data. RU jurídicos. Repositorio Universitario. UNAM. http://ru.juridicas.unam.mx/xmlui/handle/123456789/26599

Muñoz Igual, A. Las empresas Over-the-top y su impacto en el sector de las operadoras de telecomunicaciones. http://economiadigital.etsit.upm.es/wp-content/uploads/2015/12/AnaMunoz.pdf

Oberto de Grude, L. y Govea de Guerrero, M. 2008. Algunas consideraciones sobre el habeas datan en Venezuela. Télématique: Revista Electrónica de Estudios Telemáticos, ISSN-e: 1856-4194. https://dialnet.unirioja.es/servlet/articulo?codigo=2954091

Observatorio de Bioética y Derecho, Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública, Universidad de Barcelona, 2015. http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf

ONU. 50 millones de personas en el mundo en situación de esclavitud moderna. https://mexico.un.org/es/198861-50-millones-de-personas-en-el-mundo-en-situaci%C3%B3n-de-esclavitud-moderna#:~:text=GINEBRA%20%E2%80%93%20Cincuenta%20millones%20de%20personas,estaban%20atrapadas%20en%20matrimonios%20forzados.

Oracle. ¿Qué es la inteligencia artificial? Obtén más información sobre la inteligencia artificial. https://www.oracle.com/mx/artificial-intelligence/what-is-ai/

Ortiz Morales, M. D., Joyanes Aguilar, L., y Giraldo Marín, L. M. 2015. Los desafíos del marketing en la era del big data. E-Ciencias De La Información, 6(1), 1–31. https://doi.org/10.15517/eci.v6i1.19005

Paredes, A. 2021. Influencers y política 4.0. Forbes. https://www.forbes.com.mx/red-forbes-influencers-y-politica-4-0/

Parraguez Kobek, L. y Caldera, E. 2016. Cyber Security and Habeas Data: The Latin Amreican Response to Information Security and Data Protection. Oasis, no. 24, pp. 109-128. https://www.redalyc.org/journal/531/53163716007/html/index.html#B2

Patiño Orozco, G. 2021. Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos. Oasis, n-um. 34, 2021, julio-diciembre, pp. 107-126. https://www.redalyc.org/journal/531/53169476007/53169476007.pdf

Pfeiffer, M. 2008. Derecho a la privacidad. Protección de los datos sensibles. Revista Colombiana de Bioética, vol. 3, núm. 1, enero-junio, 2008, pp. 11-36. https://www.redalyc.org/articulo.oa?id=189217248002

Pons Gamón, V. 2017. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad URVIO, Revista Latinoamericana de Estadios de Seguridad, núm. 20, 2017, pp. 80-93. https://www.redalyc.org/journal/5526/552656641007/

Portabilidad de los datos personales beneficia a la ciudadanía. 2019. Infoem. https://www.infoem.org.mx/es/contenido/noticias/portabilidad-de-los-datos-personales-beneficia-la ciudadan%C3%ADa#:~:text=Ejercer%20la%20portabilidad%20de%20los,ella%2C%20afirm%C3%B3%20Javier%20Mart%C3%ADnez%20Cruz

Portela, Jorge G. 2009. Los principios jurídicos y el neoconstitucionalismo. Kíkaion, vol. 23, núm. 18, diciembre, 2009, pp. 33-54. https://www.redalyc.org/articulo.oa?id=72012329003

Primer Estudio sobre Protección de Datos Personales entre Usuarios y empresas en México. Asociación Mexicana de Internet (AMIPCI). https://irp.cdn-website.com/81280eda/files/uploaded/Microsoft%201%20Estudio%20de%20Protecci%C3%B3n%20de%20Datos.pdf

Principios Actualizados sobre la Privacidad y la Protección de los Datos Personales. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Principios y Deberes en Materia de Protección de Datos Personales. https://www.gob.mx/cms/uploads/attachment/file/763381/Principios_y_deberes_en_materia_de_Proteccion_de_Datos_Personales.pdf

Puccinelli, O. 2004. Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina. Un intento clasificador con fines didácticos. Vniversitas, núm. 107. http://www.redalyc.org/articulo.oa?id=82510714

Quijano Decanini, C. 2022. Derecho a la privacidad en Internet. México. Tirant lo Blanch.

Rebolledo, M. 2017. La personalización de la política: una propuesta de definición para su estudio sistemático. Revista de comunicación. ISSN: 1684- 0933. https://revistadecomunicacion.com/es/articulos/2017_2/7_Art.html

Recht Legal. ¿Cómo ejercer el derecho al “olvido” en México? https://recht.com.mx/ejercer/#:~:text=Los%20derechos%20ARCO%20surgen%20en,oposici%C3%B3n%20de%20sus%20datos%20personales.

Ríos Estavillo, J. 1997. Derecho e informática en México: informática jurídica y derecho de la informática/ México: Universidad Nacional Autónoma de México. http://ru.juridicas.unam.mx/xmlui/handle/123456789/9121

Risso Ferrand, M. Derecho a la propia imagen y expectativa de respeto a la privacidad. Centro de Estudios Constitucionales de Chile Universidad de Talca. ISSN: 0718 0195. https://pdfs.semanticscholar.org/eb5e/5a565ddb36918c412c0e29dc0a435977a537.pdf

Rodríguez-Andrés, R. 2018. Trump 2016: ¿presidente gracias a las redes sociales? Palabra Clave, 21(3), 831-859. https://palabraclave.unisabana.edu.co/index.php/palabraclave/article/view/8170/pdf

Romero Galicia, J. 2018. Conceptualización de una estrategia de ciberseguridad nacional en México. Revista Internacional de Ciencias Sociales y

Humanidades, SOCIOTAM, vol. XXVIII, núm. 2, 2018. https://www.redalyc.org/articulo.oa?id=65458498003

Romero Pérez, X. 2008. El alcance del derecho a la intimidad en la sociedad actual. Revista de Derecho del Estado. Bogotá, Colombia. Consultado el 14 de febrero de 2023.

Rosenber, M., Confessore, N. y Cadwalladr, C. 2018. La empresa que explotó millones de datos de usuarios de Facebook. The New York Times. https://www.nytimes.com/es/2018/03/20/espanol/cambridge-analytica-facebook.html

Save de Children. 2019. Grooming, qué es, cómo detectarlo y prevenirlo. https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

Sierra Gutiérrez, L. 2009. La cultura en la era del ciberespacio: Cibercultura. La cultura de la sociedad digital. Signo y Pensamiento, 28(54), 382-398. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-48232009000100029&lng=en&tlng=es

Soto, Y. 2017. Datos masivos con privacidad y no contra privacidad. Revista de Bioética y Derecho, (40),101-114. ISSN 1886-5887. https://www.redalyc.org/articulo.oa?id=78351101008

Suárez-Rodríguez, J. 2016. El fundamento de los principios jurídicos: una cuestión problemática. Cvilicar. Ciencias Sociales y Humanas, vol. 16, núm. 30, enero-junio, 2016, pp. 51-61. https://www.redalyc.org/articulo.oa?id=100246672002

Suprema Corte de Justicia de la Nación. Comunicados de Prensa. No. 194/2017. https://www.internet2.scjn.gob.mx/red2/comunicados/noticia.asp?id=4639

UNAM. Sexting, cuidado con tu intimidad. https://www.fundacionunam.org.mx/unam-al-dia/sexting-cuidado-con-tu-intimidad/

Vanina Carboni, O. y Labate, C. 2018. América Latina por una red neutral: el principio de neutralidad in Chile y Brasil. 2018. Revista FAMECOS: mídia, cultura e tecnologia, vol. 25, núm.2. https://www.redalyc.org/jatsRepo/4955/495557631013/html/index.html#:~:text=El%20concepto%20de%20neutralidad%20de,garantizar%20la%20conexi%C3%B3n%20entre%20usuarios.

Velasco Melo, A. H. 2008. El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. Revista de Derecho, (29),333-366. ISSN: 0121-8697.: https://www.redalyc.org/articulo.oa?id=85102913

TESIS Y JURISPRUDENCIA

Tesis 118/2013. Semanario Judicial de la Federación y su Gaceta, Décima época, Libro 3, Tomo I, febrero de 2014.

Tesis: XXX.3o.4 K (11a.). Gaceta del Semanario Judicial de la Federación. Libro 18, octubre de 2022, Tomo IV, página 3505

Tesis I.3o.C.469 C (10a.). Gaceta del Semanario Judicial de la Federación.

Tesis: I.10o.A.120 A (10a.), Gaceta del Semanario Judicial de la Federación. Libro 70, septiembre de 2019, Tomo III, página 1853.

Tesis: I.10o.A.5 CS (10a.) Gaceta del Semanario Judicial de la Federación. Libro 70, septiembre de 2019, Tomo III, página 2199

Tesis: I.10o.A.6 CS (10a.) Gaceta del Semanario Judicial de la Federación. Libro 70, septiembre de 2019, Tomo III, página 2200

Tesis 1a. V/2023 (11a.). Gaceta del Semanario Judicial de la Federación. Libro 23, marzo de 2023, Tomo II, página 2057

Tesis: 2a./J. 17/2023 (11a.). Gaceta del Semanario Judicial de la Federación. Libro 23, marzo de 2023, Tomo III, página 2236

CASOS Y SENTENCIAS

AMPARO DIRECTO EN REVISIÓN 3800/2019. RECURRENTES: GOOGLE MÉXICO, SOCIEDAD DE RESPONSABILIDAD LIMITADA DE CAPITAL VARIABLE Y GOOGLE INC. QUEJOSO: PABLO AGUSTÍN MEOUCHI SAADE.

DOCUMENTALES

Brockmann, Anija y Kroll, Katharina. (2022) Infraestructura digital crítica: ¿por qué hay cada vez más ciberataques? [vídeo]. DW español. Consultado el 28 de febrero de 2023. Disponible en: https://www.youtube.com/watch?v=bUI9oeulGAU

DW español. 2020. Viaje al lado oculto de Internet. [microdocumental] Viaje al lado oculto de Internet. https://www.youtube.com/watch?v=bZySuxR8bGM

DW español. 2023. Cómo se abusa de las aplicaciones para la esclavitud moderna. https://www.youtube.com/watch?v=l9RgxmhU1yc

López, Pablo y Gómez, Juan [productores]. ¿Cómo discrimina la inteligencia artificial? ¿Quiénes son sus víctimas? (2021). DW Español. https://www.youtube.com/watch?v=mWGzicjqAc0

Michelle Ostwald. 2021. ¿Están mis datos a la venta en la darkweb? [microdocumental]. https://www.youtube.com/watch?v=sMG9UDv6eq8

Michelle Ostwald. 2021. ¿Por qué se venden tantas drogas en la darkweb? [microdocumental]. https://www.youtube.com/watch?v=myAFhVbrIlA

NORMATIVIDAD

Código Civil del Estado de México.

Constitución de la República Bolivariana de Venezuela.

Constitución Política de los Estados Unidos Mexicanos.

Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

Ley Federal de Derechos de Autor.

Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)

Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados (LGPDPPSO)

Reglamento (EU) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.