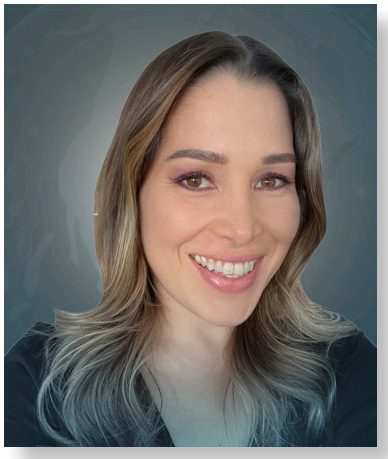
# DATOS PERSONALES Y BIOMÉTRICOS. LA APUESTA DE MÉXICO ANTE LAS TECNOLOGÍAS DE LA INFORMACIÓN

## PERSONAL AND BIOMETRIC DATA. MEXICO'S COMMITMENT WITH INFORMATION TECHNOLOGIES



**Ximena Puente de la Mora**
Doctora en Derecho por la Universidad de Guadalajara
Trabajadora e investigadora Independiente
ximenapuentecolima@gmail.com
ORCID: https://orcid.org/0000-0002-9289-072X

México

DOI: https://doi.org/10.5377/umhs.v2i1.12999

**Recibido:** 30 de agosto de 2021
**Aceptado:** 17 de noviembre de 2021

## RESUMEN

El objeto de este ensayo pretende brindar una panorámica de la importancia de la protección de datos personales, su origen en el derecho anglosajón, su desarrollo y la relevancia que han adquirido en nuestras sociedades democráticas de derecho, la interpretación latinoamericana sobre su concepto jurídico y las tendencias europeas que dan lugar al más reciente estándar normativo internacional de protección de los datos personales como derecho fundamental. En este sentido, se pretende distinguir una categoría específica a nivel internacional dentro de los datos personales, los datos especialmente protegidos o también llamados datos sensibles, específicamente los datos biométricos, y el reto que significa para los países la aplicación de la normatividad en la materia, ponderando la seguridad del manejo de la información personal, y al mismo tiempo, la necesidad creciente del intercambio de información y el flujo de esos datos.

**PALABRAS CLAVE:** Datos personales, datos biométricos, privacidad, seguridad, protección jurídica.

## ABSTRACT

The purpose of this essay aims to provide an overview of the importance of the protection of personal data, its origin in Anglo-Saxon law, its development, and the relevance it has acquired in our democratic societies of law, the Latin American interpretation of its legal concept and the European trends that give rise to the most recent international normative standard for the protection of personal data as a fundamental right. In this sense, it is intended to distinguish a specific category at the international level within personal data, specially protected data or also called sensitive data, specifically biometric data,

1 Doctora en Derecho por la Universidad de Guadalajara, Maestra en Derecho por la Universidad de Navarra y Licenciada en Derecho por la Universidad de Colima, los tres grados obtenidos con mención honorifica. Primera Presidenta del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI [2014-2017]), Organismo Constitucional Autónomo, siendo Comisionada hasta 2018. Presidenta fundadora del Sistema Nacional de Transparencia (SNT) en México (2015-2017), junto con los Organismos garantes de las Entidades Federativas, la Auditoría Superior de la Federación (ASF), el Archivo General de la Nación (AGN), y el Instituto Nacional de Estadística y Geografía (INEGI). Presidenta de la Red de Integridad, un Organismo Internacional de combate a la corrupción. Formó parte del Consejo Directivo del *Global Partnership for Social Accountability (GPSA* [2017-2018]) del Banco Mundial. Diputada Federal en la LXIV Legislatura de la Paridad de Género (2018 – 2021), Actualmente es Consultora en materia de Transparencia, Privacidad y Datos Personales. Email: ximenapuentecolima@gmail.com. Twitter: @XimenaPuente. Facebook: Ximena Puente. Instagram: Ximena Puente de la Mora, www.ximenapuente.mx

and the challenge that the application of regulations on the matter means for countries, considering the security of the handling of personal information, and at the same time, the growing need for the exchange of information and the flow of this data.

**KEYWORDS:** Personal data, biometric data, privacy, security, legal protection**.**

## INTRODUCCIÓN

Es la información la que hace funcionar al mundo, para llevar a cabo una transacción comercial, para hacer un trámite de gobierno, para realizar alguna solicitud, prácticamente cada instante de nuestra vida cotidiana, es indispensable el intercambio de información. En la presente colaboración abordaremos el derecho a la protección de datos personales, sus orígenes, implicaciones, características, la distinción con los datos especialmente protegidos, en especial los biométricos, las principales disposiciones europeas, y la apuesta jurídica de México con relación a esta materia.

## APROXIMACIÓN AL ESTUDIO DE LA PROTECCIÓN DE DATOS PERSONALES

Las sociedades democráticas de derechos han traído a la par con su evolución, beneficios y retos para los seres humanos que conviven y se desarrollan entre sí e interactúan con las instituciones del Estado, generando así prerrogativas y obligaciones que, con base al Estado de Derecho, deben cumplirse a cabalidad. La dignidad humana sirve de fundamento para sustentar a los derechos fundamentales y la obligación de reconocerlos, respetarlos y garantizar su protección por parte las autoridades, el sector privado, la sociedad civil, pero siempre con el respeto de ciertos límites como los derechos de los demás y el respecto a nuestra privacidad e información personal.

El derecho a la privacidad tiene antecedentes a finales del siglo XIX en el constitucionalismo estadounidense (Saldaña, 2012), a través de los aportes de los juristas Samuel D. Warren y Louis D. Brandeis publicados en un estudio de la *Harvard Law Review* en Diciembre de 1890 titulado "*The Rigth to Privacy*" y que consecuentemente, sentó las bases para que las y los individuos determinaran el ámbito de su vida privada que deseaban dar a conocer a terceros y el aseguramiento de que no fuesen molestados en cuanto a la publicación o la divulgación indiscriminada por parte de la prensa, todo lo relacionado con su información personal. El caso estuvo centrado en la preocupación por la difusión de fotografías instantáneas (tecnología de punta en el momento) dentro de los periódicos de la época, generando así una invasión a la vida doméstica y privada.

En sí, el derecho a la privacidad se entiende como la facultad de cada individuo de poder separar aspectos de su vida privada del escrutinio público (García, 2013); a su vez y ya dentro de un marco jurídico universal, la Declaración Universal de Derechos Humanos, que desde su aprobación por 50 países (entre ellos México), reunidos en París el 10 de diciembre en 1948, contempla el derecho a privacidad en el artículo 12 en los siguientes términos:

> 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. (United Nations, 1948)

En ese orden de ideas, "Los datos personales

es toda aquella información de una persona física que tiene como finalidad identificarla o bien hacerla identificable" (Monroy Martínez, 2017) ya sea en sistemas de archivos, almacenamiento de documentos e información de aspectos en general de uso cotidiano y que por lo tanto pueden tratar de cualquier temática (Tarango, 2013), el espectro es muy amplio, cada dato puede entenderse como una pequeña pieza de un rompecabezas que al juntarse forman un perfil muy preciso de una persona, que puede indicar rasgos no solo físicos, psicológicos, conductuales, de personalidad que están sustentados con las huellas que vamos dejando de manera cotidiana.

La protección de datos personales se relaciona con otros conceptos como privacidad, el honor, el derecho a la propia imagen derecho a la identidad.

Hoy, la sociedad digital abre caminos y oportunidades con enfoque hacia la libertad, el conocimiento, la autonomía y desarrollo de las personas, pero, también ha propiciado retos, que a su vez, diseñan y establecen vertientes y soluciones a fin de crear vías de control y vigilancia ante los inminentes riesgos, mismos que ponen en peligro o limitan los derechos y libertades fundamentales. que, como lo plantea Luigi Ferrajoli (1998) en su Teoría Garantista, son necesarios para establecer un Nuevo Modelo Normativo del Derecho y que existan limites en el actuar de las autoridades legítimamente constituidas del Estado, para lograr el ansiado equilibrio, evitar la impunidad lacerante y a su vez respetar un necesario ámbito de derechos fundamentales de los ciudadanos.

Uno de los retos que se enfrentan actualmente las sociedades y los gobiernos es la creación de reglas de conducta e instituciones que permitan organizar las transformaciones en esta nueva sociedad digital y de la información (Katz & Hilbert, 2003).

El diseño de estas instituciones, leyes y vías de solución permitirán generar resultados y relaciones positivas entre las libertades y el interés público, entre la vida privada y la información pública, la interconexión global, las identidades locales, particulares y entre el uso creciente de tecnología y la sociedad.

La entrada de los países a esta realidad marcada por el uso de la tecnología exige la adecuación de las leyes, prácticas, instituciones y la organización pública, social y empresarial al uso generalizado de las tecnologías de la información, con enfoque innovador al respeto, con la necesidad de salvaguarda y protección de la información y los datos de las personas.

Continuamente se va dejando una especie de huella digital, datos de manera cotidiana que pueden ser susceptibles de ser registrados: relojes inteligentes que miden la calidad del sueño, las horas de actividad física, la actividad cardiaca y pulmonar, a qué hora se empieza a trabajar, si se tiene hora de entrada a una oficina, cuáles son las costumbres de alimentos, de bebidas de convivencia, de productividad, cada acto que se hace o se deja de hacer es susceptible a registro que pueda ser atribuido a una persona física identificada o identificable.

A mayor uso de tecnología, mayor susceptibilidad de riesgos en el manejo y seguridad de la información personal, robo de cuentas bancarias e información de salud, por lo tanto, es de suma importancia que en las sociedades democráticas de derecho, se evalúen las opciones de brindar mayor seguridad cuando que recaben información personal, y mas aun si se trata de información biométrica, misma que con un adecuado manejo, existe la posibilidad de que contribuyan ir superando

esa barrera de inseguridad, siempre en el marco de la legalidad y la protección de las personas (Haro Antonio, 2020).

En este contexto, surge la necesidad de analizar un breve marco conceptual general sobre lo que datos personales, datos sensibles o la información especialmente protegida y datos biométricos, así como el cómo, cuándo, quién y por qué se puede solicitar, además de los retos que implican las recientes tendencias legislativas en esta materia.

La época actual esta marcada por una mercantilización de los datos personales, en las 2018 cibercriminales ponen a la venta datos personales de 120 millones de usuarios en Facebook, algunas plataformas de redes sociales permiten al usuario decidir cuales datos quieren compartir y cuales quieren proteger, en algunos países se han impuesto onerosas multas por no informar a los usuarios como comparten o venden información personal a otras compañías.

Hace falta crear una mayor conciencia por parte de las personas de los múltiples manejos de sus datos (United Nations, 2016a), poniendo en el centro del debate la necesidad de fortalecer la normativa para lograr una protección eficaz de la información personal, y evitar el aumento de cifras por ataques digitales, siendo claro ejemplo el año 2020 en donde casi 500 millones de particulares resultaron víctimas de ciberdelitos (Norton, 2019).

El creciente uso de la tecnología en la vida cotidiana y para efectos de autenticación, lleva al uso casi inminente de la biometría, explicada por el ingeniero biomédico y científico de datos de Pragma, Yorhagy Valencia, como la medida biológica o características físicas que se utilizan para el reconocimiento, autenticación e identificación de las personas (Pragma, 2019). Los datos biométricos son únicos, permiten descifrar incluso rasgos la personalidad, mismos que hacen plenamente identificable a un individuo, puesto que varían de persona a persona, y se encuentran dentro de la categoría de datos sensibles, es decir, los que su manejo inadecuado pudiera derivar en casos de discriminación.

La identidad de la biometría tiene dos vertientes una positiva, que pudiera bridar eficiencia y seguridad por medio de un proceso de autenticación seguro; y otra negativa, que amenaza con dejar un espacio muy acotado a al ámbito de privacidad (Milanés & Erreyra, 2019).

Con esto, se pretende acentuar la importancia del pleno respeto de la libertad de buscar, recibir y difundir información, incluida la importancia fundamental del acceso a la información y la participación democrática, recordando que el derecho a la privacidad, la libertad de expresión y la libertad de acceso a la información contribuyen al libre desarrollo de la personalidad y que la tecnología digital pudiera tener impacto en el disfrute de estos derechos.

Proteger los datos personales aporta a preservar y proteger la autodeterminación informativa de las personas, tal como lo declara la sentencia de 15 de diciembre de 1983, del Tribunal Constitucional Federal Alemán (Schwabe, 2009). El intercambio de información personal debe considerarse como un elemento transversal a diversas esferas en las que se desempeñan las personas.

De acuerdo con una investigación de *British Broadcasting Corporation* (BBC) publicada por Portafolio, el mercado global de las tecnologías biométricas alcanzará los US$ 41.500 millones para el 2020 (Campillo, 2021), así mismo estos sistemas

puede suponer un gran apoyo en la seguridad digital de las empresas, mejorando su control en materia ataques a la identidad puesto que los ciberdelincuentes suelen aprovechar la información disponible. Ejemplo de ello es que el 63% de los accesos por los hackers a la red es causa de un mal uso de las contraseñas y nombres de usuario (Zaharia, 2021).

Estas son solo algunas cifras que muestran la necesidad de regular la utilización de datos biométricos con el objeto de que pueda avanzar la regulación jurídica a la par del inminente avance tecnológico.

Es por ello resulta necesario en la sociedad, la existencia de estructuras que encuadren las acciones del Estado y de los particulares dentro de la legalidad respetando en todo momento los derechos fundamentales; sin privacidad, no hay democracia.

## MARCO CONCEPTUAL DE DATOS PERSONALES, SENSIBLES Y BIOMÉTRICOS

Se debe garantizar el espectro de derechos fundamentales de las personas, incluido el derecho a la privacidad, cualquier limitación de este derecho debe respetar los principios generales de legalidad, necesidad y proporcionalidad (United Nations, 2016b).

Los avances tecnológicos están cada vez mas presentes en la vida cotidiana, desde controlar el a los centros de trabajo, para impedir accesos no autorizados a las instalaciones, controlar los horarios y presencia, es cada vez mas común el uso de los datos biométricos como el reconocimiento facial, la huella dactilar, el tono de voz, el iris de los ojos.

Los datos personales se refieren a toda información que es perteneciente a una persona física identificada o identificable y es contenida en archivos y/o bases de datos; estos datos pueden tomar la clasificación de sensibles cuando 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 (Instituto de Investigaciones Jurídicas, UNAM, 2020).

Debido a su naturaleza es que, dentro de los datos sensibles, se sitúan los datos biométricos, mismos que exigen un marco de control exhaustivo y delimitado que se debe cumplir rigurosamente, sobre todo en el necesario nivel de seguridad que exigen, y el consentimiento informado sobre el uso y destino de los mismos.

En el mismo sentido, es importante resaltar que la información biométrica puede ser utilizada por las autoridades para cumplir de mejor manera con sus facultades y para proveer mejores servicios a la ciudadanía., bajo un estricto criterio legalidad, proporcionalidad y necesidad

Es por ello que, los derechos de información, intimidad, privacidad, ampliamente vinculados, pero con características específicas cada uno de ellos, deben ser especialmente protegidos ante el uso creciente de las tecnologías de información y comunicación (TIC); ya que se trata de derechos fundamentales, con lo que su vulneración o transgresión puede conllevar lesiones a la esfera más personal de un individuo.

En este ámbito, el 25 de mayo de 2018, entró en vigor el nuevo Reglamento General de Protección de Datos Europeo (RGPD); se considera como uno de los estándares más alto de protección

de la información personal, establece obligaciones específicas de cumplimiento lo los países miembros para la protección, cuidado y seguridad en el tratamiento de Datos Personales y Datos Personales Sensibles, así como de los países que busquen el reconocimiento por parte de la Unión Europea como Nivel Adecuado de Protección de Datos, para las transferencias internacionales, en Latinoamérica tienen este reconocimiento Argentina y Uruguay, México está trabajando con las autoridades europeas para conseguir esta certificación.

En el Reglamento Europeo hace referencia que **los datos sensibles** revelan: origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, filiación sindical, datos genéticos, datos biométricos con el objetivo de identificar de manera exclusiva a un individuo, datos relativos a la salud o la vida sexual y/o la orientación sexual.

Establece también a los datos biométricos como: "Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

Los datos biométricos son las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles:

- Universales, ya que son datos con los que contamos todas las personas;
- Únicos, ya que no existen dos biométricos con las mismas características por lo que nos distinguen de otras personas;
- Permanentes, ya que se mantienen, en la mayoría de los casos, a lo largo del tiempo en cada persona, y Medibles de forma cuantitativa (Parlamento Europeo, 2016).

Entre los datos biométricos que refieren a características físicas y fisiológicas se encuentran la huella digital, el reconocimiento facial, la retina, el iris, la geometría de la mano o de los dedos, la estructura de las venas de la mano, la forma de las orejas, la piel o textura de la superficie dérmica, el ADN, la composición química del olor corporal y el patrón vascular, pulsación cardíaca, entre otros (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos, INAI 218).

## LA UNIÓN EUROPEA Y EL DERECHO FUNDAMETAL A LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL.

La protección de los datos personales y el respeto de la vida privada son derechos fundamentales contemplados en los sistemas jurídicos europeos. El inicio de la regulación de los datos personales en se remonta al Estado de Hesse en Alemania en 1970, con una regulación de carácter local y cuyo objeto era brindar protección a las personas físicas ante la amenaza que representaba el tratamiento automatizado de datos nominativos por las autoridades y administraciones públicas del Estado, los municipios y entidades locales rurales, así como las demás personas jurídicas de derecho público y agrupaciones sujetas a la tutela estatal (Universidad de Chile Facultad de Derecho & Centro de Estudios en Derecho Informático, 2003); esta ley local dio la pauta para la creación y promulgación de las leyes nacionales en Suecia durante 1973, Alemania en 1977 y Francia en 1978.

De ahí también señalar el pronunciamiento del

Tribunal Constitucional Alemán el 15 de diciembre de 1983 en esta materia, al declarar inconstitucional la del Censo de 1983, en donde por primera vez se habla de un derecho de autodeterminación informativa, al señalar este alto tribunal que las limitaciones a este derecho solo son admisibles en el marco de interés general superior y necesitan un fundamento legal basado en la Constitución, la clave de este ordenamiento se encuentra en el valor y la dignidad de la persona.

Señala también este Máximo Tribunal Constitucional alemán, que es una facultad del individuo derivada de la autodeterminación, decidir básicamente cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida. Como se puede observar ésta importante decisión judicial, delimita el ámbito del derecho a la protección de datos personales o el derecho a la autodeterminación informativa. La tecnología sin duda ha avanzado mucho en las últimas décadas, pero los principios jurídicos es la decisión del propio individuo con base a su inherente dignidad, decidir en qué medida desea compartir su vida personal y las herramientas del Estado para poder respetar y proteger esta decisión.

Posteriormente, el Consejo y el Parlamento Europeos (1995) con base al Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, adoptan la Directiva 95/46/CE relativa a la protección de las personas físicas respecto al tratamiento de sus datos personales y la libre circulación de estos, a fin de obligar a los Estados miembros la protección de la vida privada con enfoque en el tratamiento de datos personales.

La Directiva crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (Unión Europea, 2014).

Se fijan los límites para la recoger y tratar datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional autónomo que supervise toda actividad relacionada con el tratamiento de los datos personales.

Así, es como el Parlamento Europeo ha insistido en la necesidad de lograr un equilibrio entre el refuerzo de la seguridad y la tutela de los derechos humanos, incluida la protección de los datos y de la vida privada.

Las nuevas normas de la Unión en materia de protección de datos, que refuerzan los derechos de los ciudadanos y simplifican las normas para las empresas en la era digital, entraron en vigor en mayo de 2018.

El nuevo Reglamento General de Protección de Datos Europeo (RGPD según sus siglas en español), fue aprobado el 27 de abril de 2016, aunque su entrada en vigor no se produjo hasta el 25 de mayo de 2018.

El objetivo central del RGPD, es garantizar la aplicación sistemática del derecho fundamental a la protección de datos, consagrado en la Carta de los Derechos Fundamentales de la Unión Europea, reforzando la posición de la Unión sobre la protección de los datos personales en el marco de todas sus políticas, incluidas la aplicación de la ley y la prevención de la delincuencia, así como en sus relaciones internacionales, especialmente en una sociedad global caracterizada por la rápida evolución de la tecnología (Maciejewski, 2021).

El RGPD representa un valioso instrumento unificador más que una directiva, a diferencia de

su predecesora y a la cual deroga, la Directiva de Protección de Datos de 1995 95/46/EC; en la cual a cada país le correspondía diseñar sus propias leyes de protección de datos de forma individual. Por ello, las empresas y organizaciones que operan a lo largo y ancho de diferentes países de la alianza europea se encontraron inmersas en todo un gran laberinto legal formado por múltiples leyes.

Afortunadamente, el RGPD reemplaza esta complejidad con una sola ley unificada que simplifica significativamente la gestión para las empresas, establece un estándar normativo más sólido también para los Estados miembros y para los países con los que tengan flujo transfronterizo de datos, y a las empresas extranjeras que tenga información personal de ciudadanos europeos, así como de establecer un marco de seguridad para el desarrollo de un mercado digital mediante la creación de nuevos servicios, aplicaciones, plataformas y software.

Dentro de los aspectos relevantes del RGPD, se encuentran:

1. La obtención del consentimiento para el tratamiento de datos debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen.

2. El RGPD reconoce a las personas físicas derechos sobre sus datos personales y establece fórmulas y mecanismos para solicitar y, en su caso, obtener gratuitamente el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición.

3. Según el RGPD, las empresas y los terceros que procesen datos personales en su nombre designarán un delegado de protección de datos (DPD) siempre que:
– Se trate de una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial,
– Las actividades principales de la empresa o el tercer consistan en la observación de interesados a gran escala; o
– Sus actividades principales consistan en el tratamiento a gran escala de datos personales sensibles, como los datos relativos a condenas o infracciones penales.

4. Las organizaciones que habitualmente realicen un tratamiento de datos de riesgo para la privacidad de los interesados o traten datos sensibles, deben llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

5. La entrada en vigor del Reglamento General de Protección de Datos (RGPD), incrementa significativamente las sanciones que se derivan del incumplimiento, dependiendo del artículo del Reglamento General de Protección de Datos que se haya vulnerado, infracciones que van de los 10 millones a 20 millones de euros como máximo. Además de las multas administrativas, el reglamento prevé que las sanciones puedan implicar también la prohibición del tratamiento de datos o la suspensión de las transferencias internacionales de datos.

El 28 de enero de 1981 el Consejo

de Europa adoptó el Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, o Convenio 108 del Consejo de Europa el cual constituye un marco de referencia para diversos países en materia de datos personales. El objetivo del Convenio 108 es crear una armonía entre el tratamiento de datos personales y el libre flujo de los datos para el mejoramiento del comercio entre los países. Este equilibrio puede lograrse basándose en principios que todos los Estados puedan reconocer y aplicar de acuerdo con el Convenio. Es vinculatorio para 55 países, México es miembro de este instrumento internacional desde el 12 de junio de 2018.

La necesidad de actualizar las normas impulsa el Convenio 108+ mismo que se abre a firma el 10 de octubre en Estrasburgo, y clarifica las bases legales sobre las cuales se pueden tratar datos personales, se amplía el catálogo de datos sensibles, se obligan a notificar las brechas de seguridad que afecten a los individuos, se facilitan las transferencias de datos, siempre que se hagan respetando estos niveles de seguridad.

Ahora bien, es importante analizar la influencia del derecho a la protección de datos personales, nacido en Europa y proyectado en las últimas décadas en otras zonas geográficas como América Latina.

La protección de datos personales está viviendo en la actualidad un periodo de cambio profundo, tanto en Iberoamérica como en EE. UU. y en la Unión Europea. Los países iberoamericanos están afrontando en los últimos años un proceso de aprobación de normas de protección de datos personales, que gradualmente, aproxima su legislación al modelo europeo.

Como es sabido, la protección de los datos personales dentro del modelo americano ha descansado hasta ahora en la autorregulación vinculante y en el ámbito del derecho del consumo y del derecho de la competencia. Las empresas tienen que cumplir con sus clientes sus compromisos de privacidad y si no lo hacen se les puede exigir judicialmente su responsabilidad y la correspondiente indemnización. En cambio, el modelo europeo de protección de datos ha apostado por las herramientas normativas heterónomas, de ahí su fuerte asimetría con el modelo americano (Troncoso Reigada, 2018).

Los países iberoamericanos han reconocido en sus Constituciones el derecho fundamental a la protección de los datos personales y han ido aprobando leyes generales de protección de datos personales, a consecuencia en gran medida de los diversos estándares emanados de la Unión Europea quien, aun sin proponérselo, están sirviendo como base para la regulación de la materia a nivel global (López-Torres, 2014).

## PERSPECTIVA Y AVANCES EBN AMÉRICA LATINA; LA APUESTA DE MÉXICO EN LA ERA DIGITAL.

En los últimos años, un número significativo de países de Latinoamérica ha ido incorporando no sólo una legislación específica en materia de protección de datos personales sino también, un conjunto de instrumentos organizativos y legales

para asegurar unas garantías adecuadas y suficientes y, en consecuencia, una protección efectiva para los ciudadanos (García González, 2015).

En ese sentido y en aras de fomentar el pleno respeto y salvaguarda de la privacidad y la protección de los datos personales, el Comité Jurídico Interamericano (CJI), como órgano consultivo de la Organización de los Estados Americanos (OEA) en asuntos jurídicos, en Abril del 2021 concluyó su 98º periodo ordinario de sesiones aprobando una serie de principios sobre la Privacidad y la Protección de los Datos Personales (Comité Jurídico Interamericano, 2021), con el único objetivo de que los países de América conozcan y adopten la importancia de regular en materia de protección a la privacidad de su ciudadanía, invitándolos a que armonizasen sus leyes en el tenor y a la luz de los principios emitidos

La actualización de los Principios atiende concretamente a que el tratamiento de los datos esta inminentemente expuesto a las nuevas aplicaciones digitales y por lo tanto los controladores y encargados de los datos, tendrán que optar por establecer medidas de seguridad sobre todo enfocadas a los datos personales sensibles, su flujo transfronterizo, el consentimiento de los ciudadanos y el respecto en tratamiento de su información.

La Corte Interamericana de Derechos Humanos, es uno de los tres tribunales regionales de protección de los derechos humanos, En conjunto con la Corte Europea de Derechos Humanos y la Corte Africana de Derechos Humanos y de los Pueblos. Es una institución judicial autónoma cuyo objetivo es aplicar e interpretar la Convención Americana. La Corte Interamericana ejerce una función contenciosa, dentro de la que se encuentra la resolución de casos contenciosos y el mecanismo de supervisión de sentencias; una función consultiva; y la función de dictar medidas provisionales.

Son veinte los Estados que han reconocido la competencia contenciosa de la Corte, dentro de los cuales se encuentran Honduras y México. Dentro de las funciones de la Corte Interamericana de Derechos Humanos, en adelante IDH, es determinar si un Estado ha incurrido en responsabilidad internacional por la violación de alguno de los derechos consagrados en la Convención Americana o en otros tratados de derechos humanos aplicables al Sistema Interamericano.

Por su parte, México en su Constitución, tiene reconocidos como derechos humanos o fundamentales (Carbonell & Comisión Nacional de los Derechos Humanos, 2004) aquellos que están íntimamente relacionados con el acceso a la información (artículo 6), la libertad de expresión y de imprenta (artículo 7), la protección de datos personales (artículo 16); y la inviolabilidad de las comunicaciones (artículo 16).

El Contenido constitucional da las bases para que en México se brinde una atención especial al acceso a la información de las personas, al seguimiento del uso de los recursos públicos y a la protección de los datos personales, tutelados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), organismo con autonomía constitucional, especializado, colegiado, independiente, imparcial, transparente y profesional.

Por su parte la Suprema Corte de Justicia de la Nación, en México (en adelante SCJN), ha emitido diversos criterios a fin de concretar una efectiva regulación de la protección de los datos personales, interpretando las normas relativas a la protección de este derecho, definiendo su alcance.

En ese orden de ideas, destaca lo que la SCJN ya ha establecido en relación a la protección de datos personales y su relación con las nuevas tecnologías, y es que se estableció el 6 de septiembre del 2019 en la tesis: I.10o.A.6 CS (10a.) la cual señala el deber por parte del Estado Mexicano frente al derecho de las y los gobernados a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de la sociedad, y que conlleva la obligación de dejarlos exentos e inmunes a invasiones por parte de terceros o de la autoridad pública, debe potencializarse ante las nuevas herramientas tecnológicas (Camero Ocampo & Suprema Corte de Justicia de la Nación, 2019b).

Otro criterio establecido por el Supremo Tribunal de Justicia en México a través de la Tesis I.10o.A.5 CS (10a.) la cual establece que la protección de los datos personales constituye un derecho vinculado con la salvaguarda de otros derechos fundamentales inherentes al ser humano en razón de que el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce los denominados derechos de Acceso, Rectificación, Cancelación u Oposición de datos personales, como un medio para garantizar el derecho a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de la sociedad, y la posibilidad de exigir su cumplimiento a las autoridades y particulares que conocen, usan o difunden dicha información (Camero Ocampo & Suprema Corte de Justicia de la Nación, 2019b).

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 Constitución y por lo tanto se tiene la obligación de garantizar y proteger el derecho de todo individuo a no ser interferido o molestado en ningún aspecto de su persona como el honor, intimidad, o los que permiten el desarrollo integral de su personalidad como ser humano.

México a fin de garantizar el mayor y amplio cumplimiento de los principios constitucionales y en pro de atender a los mandatos internacionales en materia de protección de datos personales, ha establecido que su marco jurídico se comprenda por dos rubros específicos, es decir, para regular el actuar de entes públicos se estableció una Ley General de Protección de los Datos Personales en Posesión de los Sujetos Obligados y para regular a entes privados, se cuenta con una Ley Federal de Protección de Datos Personales Posesión Particulares.

Estas Leyes Secundarias y reglamentarias del párrafo segundo del artículo 16 Constitucional, tienen como objeto principal, garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados o en posesión de particulares, regulando el tratamiento de manera legitima, controlada e informada.

Ambas leyes también se encargan de establecer un tratamiento especial y diferenciado respecto de los datos sensibles, definiendo en el artículo 3, fracción X y fracción VI, respectivamente, a estos datos como

> [A]quellos 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 este. De manera enunciativa, mas 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, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Estas leyes también destacan la ausencia de definición de Datos Biométricos, a pesar de que en la actual LXIV Legislatura, se impulsaron reformas a fin de comenzar la subsanación de esta laguna jurídica; La Cámara de Diputados Federal el 3 de febrero del 2021, aprobó en su Pleno reformar la fracción X del artículo 3 de la Ley General de Protección de los Datos Personales en Posesión de los Sujetos Obligados para especificar que, los datos personales sensibles, aparte de los ya enunciados, también serán aquellos que comprenden a las convicciones religiosas, la afiliación sindical, información relativa a la preferencia u orientación sexual, información genética o biométrica dirigida a identificar de manera unívoca a una persona física. Esta abre la posibilidad de ello al incluir y visibilizar esta importante categoría en la ley.

En México, el Instituto Autónomo garante de esta materia el INAI en 2018 emitió una Guía para el Tratamiento de Datos Biométricos, documento no vinculante, pero sin duda importante para la consulta y de referencia para orientar a las autoridades públicas y privadas en el correcto tratamiento de los datos biométricos, mismos que define en su Glosario de Términos como las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles, entre las que la huella digital, el rostro, la retina, el iris, la geometría de la mano o de los dedos, la estructura de las venas de la mano, la forma de las orejas, la piel o textura de la superficie dérmica, el ADN, la composición química del olor corporal y el patrón vascular, pulsación cardiaca, entre otros (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI, 2018)

Otro Avance reciente que se traduce como otro acercamiento a definir, regular y garantizar la protección de los datos biométricos es la iniciativa con proyecto de Decreto por el que se expide la Ley General de Población y se abroga la Ley General de Población, publicada en el Diario Oficial de la Federación el 7 de enero de 1974, aprobada el 3 de diciembre de 2020 por el Pleno de la Cámara de Diputados y turnada a la Cámara de Senadores, en donde actualmente se encuentra en estudio para su eventual discusión y votación.

Es en este nuevo proyecto en donde el Poder Legislativo a buscado establecer y dar cierta relevancia a los datos biométricos como herramienta para identificar a las y los mexicanos ya que en su Título Cuarto del Registro Nacional de Población e Identificación Personal, Capítulo I, Sección Primera, artículo 47, se señala que el Registro Nacional de Población, administrado por la Secretaría de Gobernación, será el sistema de información que contendrá los datos personales de las y los ciudadanos, incluidos los datos biométricos y que a su vez son definidos en su artículo 4, Fracción VIII como aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas o fisiológicas de una persona física que permitan distinguir confirmar fehacientemente la identidad única de la persona.

El proyecto también propone crear la Cédula Única de Identidad Digital, la cual deberá contener tanto física como digitalmente la Clave Única de Registro de Población o CURP, Nombre completo, fecha de nacimiento, nacionalidad y los datos biométricos y estableciendo en el artículo 67 que la persona titular de la Cédula es responsable de la custodia, conservación y actualización de toda la información contenida en ella.

En el mismo contexto, con importancia a

nivel internacional y de reciente reconocimiento es el Tratado Comercial entre los Estados Unidos de América, los Estados Unidos Mexicanos y Canadá (T-MEC) mismo entró en vigor el 1 de julio del 2020.

En el Capítulo 19, se regula lo relativo al Comercio digital con un enfoque dirigido a la protección tanto de las transacciones comerciales de las partes y la protección de sus Datos Personales, al enunciar en su Artículo 19.8 que la protección de la información personal de los usuarios del comercio digital es plenamente reconocida.

Este capítulo subraya la importancia de asegurar el cumplimiento de las medidas para proteger la información personal y asegurar que las restricciones a los flujos transfronterizos de información personal son necesarias y proporcionales a los riesgos presentados en las prácticas comerciales.

A su vez, establece parámetros a fin de garantizar la ciberseguridad de las y los ciudadanos de Norteamérica, al regular en su artículo 19.11 la transferencia transfronteriza de información por medios electrónicos, así como que ningún país prohibirá o restringirá la transferencia transfronteriza de dicha información por medios electrónicos, cuando la actividad sea para realización de negocio de una persona cubierta.

Contempla la importancia de la ciberseguridad en el Artículo 19.15, visibilizando las eminentes amenazas electrónicas y busca fortalecer acciones, mecanismos y desarrollar capacidades.

Otro cambio jurídico reciente y que abona en materia de la información biométrica en México es la reciente reforma Ley Federal de Telecomunicaciones publicada en el Diario Oficial de la Federación el 16 de Abril del 2021 y que en ella se crea el Padrón Nacional de Usuarios de Telefonía Móvil y por lo tanto, legitima al Instituto Federal de Telecomunicaciones para estar a cargo de instalar, operar, regular, mantener su buen funcionamiento y el intercambio de información con las demás autoridades.

El Padrón Nacional de Usuarios de Telefonía Móvil deberá contener información sobre el número de línea telefónica móvil, la fecha y hora de la activación de la línea telefónica móvil adquirida en la tarjeta SIM, el nombre completo o, en su caso, denominación o razón social del usuario, su nacionalidad, el número de identificación oficial con fotografía o CURP del titular de la línea, los Datos Biométricos del usuario o del representante legal de la persona moral, el domicilio del usuario, entre otros, estableciendo que el registro de esta información en el Padrón Nacional de Usuarios de Telefonía Móvil será de carácter obligatorio para el usuario.

Con este cambio, México se enlista junto con otros 17 países que contemplan en sus leyes el registro de datos biométricos asociados a tarjetas SIM; estos países son Afganistán, Arabia Saudita, Bahréin, Bangladesh, Benín, China, Nigeria, Omán, Pakistán, Perú, Singapur, Tayikistán, Tanzania, Tailandia, Uganda, Emiratos Árabes Unidos y Venezuela.

Los altos costos de llevar a cabo un proyecto de dicha magnitud, los riesgos de la vulneración de derechos humanos, la protección de datos personales, privacidad, incluso la limitación de las comunicaciones de quienes no dieran su consentimiento para recabar su información biométrica, hizo que en Octubre de 2021, la Primera Sala de la Suprema Corte de Justicia de la Nación suspendiera indefinidamente la elaboración de este Padrón Nacional de Usuarios de Telefonía Móvil, en tanto el Plano de este Máximo Tribunal resuelve su Constitucionalidad.

En Latinoamérica se tiene un enorme reto de proteger la información biométrica y los datos personales de millones de personas, incrementar el conocimiento de la importancia que tiene la información personal, sector público y privado implementar estrictos niveles de seguridad, notificar a todos los usuarios brechas de seguridad que se detecten, notificar los alcances de las mismas y que medidas se deben tomar para contrarrestar los efectos, pero también para evitar que vuelvan a suceder.

## CONCLUSIONES

Es un hecho que el tema de la protección de la información personal contenida en diversas bases de datos cobra una mayor importancia, para el Estado, para el sector privado, pero aun más para la sociedad que utiliza la tecnología de manera creciente en la vida diaria.

Las autoridades alrededor del mundo también han reconocido la importancia de la debida protección a la privacidad, por lo que han emitido regulaciones estrictas para la obtención y tratamiento de datos personales. Sin embargo, las cifras por robo de identidad en el mundo crecen de manera significativa, la Comisión Federal de Comercio en Estados Unidos recibió 1.4 millones de denuncias en el 2020, cifra que representa el doble que el año anterior. Argentina por ejemplo medios locales afirman que el robo de identidad fue una de más modalidades de ciberdelito que más creció en 2020, mientras que en México es uno de los delitos con mayor crecimiento.

El manejo de información personal se vuelve cada vez mas estratégico en la sociedad, en las empresas para el control de sus clientes, conocimiento de sus preferencias e incluso para predecir sus preferencias. Para el sector público, cada vez son mas necesarios para realizar todo tipo de trámites. Resulta indispensable tener una mayor conciencia de la ciudadanía respecto al valor de los datos y de como los podemos proteger y al mismo tiempo traducir las disposiciones legales existencias en confianza y seguridad para el manejo debido de la información personal de todas y de todos.

Es indispensable el trabajo y colaboración conjunta, sector público, privado, la academia, la sociedad para lograr una verdadera sociedad de derechos, en donde sea posible el avance tecnológico, pero al mismo tiempo la seguridad jurídica y el respeto a los derechos fundamentales.

## BIBLIOGRAFÍA

Camero Ocampo, J. & Suprema Corte de Justicia de la Nación. (2019a, abril 25). *Protección de Datos Personales. Constituye un derecho vinculado con la salvaguarda de otros derechos fundamentales inherentes al ser humano.* Semanario Judicial de la Federación.

Camero Ocampo, J. & Suprema Corte de Justicia de la Nación. (2019b, mayo 25). *Protección de Datos Personales. El deber del estado de salvaguardar el derecho humano relativo debe potencializarse ante las nuevas herramientas tecnológicas, debido a los riesgos que éstas representan por sus características.* Semanario Judicial de la Federación.

Campillo, R. (2021). *Estadísticas sobre biometría para 2021. Mercado y sectores*. Mobbeel.

Carbonell, M. & Comisión Nacional de los Derechos Humanos. (2004). *Los derechos fundamentales en México*. Universidad Nacional Autónoma de México.

Comité Jurídico Interamericano. (2021). *Informe del Comité Jurídico Interamericano.*

*Principios actualizados del comité jurídico interamericano sobre la privacidad y la protección de datos personales*. Organización de Estados Americanos.

Congreso de la Nación Argentina. (2000). *Ley 25.326 de Protección de Datos Personales*. Argentina.

Congreso Nacional de Chile. (1999). *Ley Chile -19628*.

Convenio número 108 del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM.

Ferrajoli, L. (1998). *Derecho y Razón. Teoría del Garantismo Penal*. Trotta.

García, D., Instituto de Investigaciones Jurídicas, UNAM, Suprema Corte de Justicia de la Nación, & Fundación Konrad Adenauer. (2013). *Artículo 16 Constitucional, Derecho a la Privacidad*. Biblioteca Jurídica Virtual UNAM.

García González, A. (2015). *Protección de Datos y Habeas Data: Una Visión Desde Iberoamérica*. Agencia Española de Protección de Datos.

Haro Antonio, C. N., Vicario Solorzano, C. M., & Instituto Politécnico Nacional. (2020). *Dispositivos biométricos para seguridad*. Boletín UPIITA El camino de la innovación educativa. Instituto Politécnico Nacional.

INAI. (2018, marzo). *Guía para el Tratamiento de Datos Biométricos*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

INEGI. (2020, 14 mayo). *Estadísticas a propósito del Día Mundial del Internet*. Instituto Nacional de Estadística y Geografía.

Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México. (2020, 10 abril). ¿Qué son los datos personales sensibles? Guía Jurídica por Afectaciones Derivadas del COVID-19. UNAM.

Katz, J. M., & Hilbert, M. R. (2003). *Los caminos hacia una sociedad de la información en América Latina y el Caribe*. Comisión Económica para América Latina y el Caribe CEPAL.

López-Torres, J. (2014, 25 noviembre). Antecedentes internacionales en materia de privacidad y protección de datos personales. Ejil - EAFIT Journal of International Law. Universidad EAFIT Revistas Académicas.

Maciejewski, M. (2021, mayo). *La protección de los datos personales*. Fichas temáticas sobre la Unión Europea y el Parlamento Europeo.

Milanes, V., & Erreyra, E. (2019). *Encuentro Iberoamericano de Protección de Datos Personales y 4to. Foro Internacional de Datos* (XVII). Asociación por los Derechos Civiles.

Monroy Martinez, C. & Universidad Nacional Autónoma de México. (2017, 21 marzo). La UNAM y la Protección de Datos Personales [Diapositivas]. UNAM.

Norton. (2019). *Informe sobre ciberseguridad de NortonLifeLock*.

Parlamento Europeo. (2016, 27 abril). *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. EUR-LEX.Europa.Eu.

Parlamento Europeo & Consejo de Europa. (1995, 24 noviembre). Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Eur-Lex.

Pandemia y Derechos Humanos en las Américas, resolución 1/2020, OEA abril 2020. Organización de Estados Americanos.

Schwabe, J. (2009). *Jurisprudencia del Tribunal Constitucional Federal Alemán. Extractos de las sentencias más relevantes*. Jurisprudencia del Tribunal Constitucional Federal Alemán. Programa de Estado de Derecho para Latinoamérica. Fundación Konrad Adenauer.

Tarango, J. & Universidad Complutense de Madrid. (2013, 4 septiembre). La información personal en la era digital. *Documentación de las Ciencias de la Información*, *36*.

Tratado Entre Los Estados Unidos Mexicanos, Los Estados Unidos De América Y Canadá, T-MEC, capítulo 19 Comercio Digital.

Troncoso Reigada, A. (2018). El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel internacional. *Revista Latinoamericana de Protección de Datos Personales*, *Número 5*.

Unión Europea. (2014, 8 marzo). Protección de los datos personales. Publications. European Union.

United Nations. (1948, 18 diciembre). *La Declaración Universal de Derechos Humanos. Naciones Unidas*. ONU.

United Nations. (2016, 31 octubre). *El derecho a la privacidad en la era digital*. Asamblea General de las Naciones Unidas. ONU.

Facultad de Derecho & Centro de Estudios en Derecho Informático. (2003). Autodeterminación informativa y leyes sobre protección de datos. *Revista Chilena de Derecho Informático*. Universidad de Chile.

Villa Bedolla, H. (2020). Reconocimiento y protección de los datos personales biométricos en México. *Revista del Centro de Estudios de Derecho e Investigaciones Parlamentarias «Quórum 132 Legislativo»*, 11–74. Cámara de Diputados del H. Congreso de la Unión.

Zaharia, A. (2021, 29 junio). *300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends*. Comparitech.