UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

DIVISIÓN DE ESTUDIOS DE POSGRADO

COMPARATIVA DE LAS LEYES DE PROTECCIÓN DE DATOS ENTRE EUROPA, ESPAÑA Y MÉXICO EN TORNO A LOS DATOS BIOMÉTRICOS

Tesis para obtener el grado de Maestro en
Derecho de la Información

Presenta:

LIC. GADADHAR NARAYANA PÉREZ ANDRÉS

DIRECTOR DE TESIS:

Mtro. ALBERTO CASIMIRO ANDRADE

Morelia Michoacán, agosto del 2022

DEDICATORIA

A mi maestro Bhakti Nirmal Acharyya,
quien en todo momento me dio apoyo,
inspiración y fuerza para continuar adelante
en este mundo lleno de problemas,
pero también de soluciones

A mi familia quienes siempre han estado ahí,
incondicional y afectuosamente apoyándome
en las buenas y en las malas

A mi esposa e hijos quienes han sido el pilar
de mi inspiración para la realización de esta tesis
y de muchas más que sirvan al progreso de la sociedad.

AGRADECIMIENTO

A mi patria la República Mexicana quien me permitió nacer, crecer y educarme, y que me ha inspirado y protegido durante estos años de vida. A CONACYT quien ofrece indistintamente oportunidades de superación profesional a todas las personas. A la Universidad Michoacana de San Nicolás de Hidalgo, a través de la Facultad de Derecho y Ciencias Sociales, que mediante la División de Estudios de Posgrado me permitió continuar con mis estudios y preparación académica.

A mis profesores, compañeros y trabajadores en general de la Universidad Michoacana, que con su esmero y dedicación, crearon un ambiente propicio para culminar la maestría sobre Derecho de la Información. A todos, gracias.

ÍNDICE

ÍNDICE DE TABLAS

Capítulo II.

RESUMEN

Los datos biométricos en la época digital retoman una vital importancia debido al negocio que surge del tratamiento masivo de datos personales por parte de particulares y entidades financieras, sobre todo por la vulnerabilidad que pueden sufrir los titulares a su privacidad durante el proceso de tratamiento. Es por ello que resulta imprescindible el que exista su reconocimiento expreso y regulación en las leyes de protección de datos. Sería imprescindible para su blindaje jurídico y además, provocar el efecto jurídico de promover la cultura de protección de datos y privacidad entre los entes económicos y entidades financieras, sobre todo el que su utilización se limite a los casos estrictamente necesarios y que su uso vaya siempre acompañada de una justificación plena, tal como se exige en la Unión Europea y España.

A través de un conocimiento amplio de su conceptualización, historia, generalidades de funcionamiento del sistema biométrico, referencias de regulación en diversos países y la comparativa de leyes de protección datos entre Europa, España y México, se pretende abordar cuáles son los aspectos que se puedan tomar en cuenta al momento de actualizar la ley mexicana de protección de datos a cargo de particulares en torno al reconocimiento de los datos biométricos como especialmente sensibles, donde sin duda alguna deba actualizarse en conjunto con el reconocimiento de los derechos digitales, ya que éstos amplían el espectro de protección de los mismos en el entorno digital, siempre respecto a garantizar los derechos a la personalidad, tal como el derecho a la autodeterminación informativa.

Palabras clave: Biometría, datos biométricos, privacidad, datos personales, datos sensibles, tratamiento de datos, particulares, titulares, sistemas biométricos, ciberseguridad, ética digital, derechos a la personalidad

ABSTRACT

Biometric data in the digital age is once again of vital importance due to the business that arises from the massive processing of personal data by individuals and financial entities, especially due to the vulnerability that data subjects may suffer from their privacy during the processing process. That is why it is essential that there is express recognition and regulation in data protection laws. It would be essential for its legal shielding and, furthermore, to cause the legal effect of promoting a culture of data protection and privacy among economic entities and financial entities, especially that its use is limited to strictly necessary cases and that its use is always accompanied by a full justification, as required in the European Union and Spain.

Through a broad knowledge of its conceptualization, history, generalities of the operation of the biometric system, regulatory references in various countries and the comparison of data protection laws between Europe, Spain and Mexico, it is intended to address what are the aspects that can be take into account when updating the Mexican data protection law in charge of individuals regarding the recognition of biometric data as especially sensitive, where without a doubt it must be updated in conjunction with the recognition of digital rights, since these expand the spectrum of protection of the same in the digital environment, always with respect to guaranteeing the rights to personality, such as the right to informative self-determination.

Keywords: Biometrics, biometric data, privacy, personal data, sensitive data, data processing, individuals, holders, biometric systems, cybersecurity, digital ethics, personality rights

INTRODUCCIÓN

En la actual época digital, los datos, y en particular los especialmente sensibles, han obtenido un valor económico sin precedentes. Algo que se está convirtiendo en uno de los activos más importantes para cualquier organización en el siglo XXI, como un verdadero motor de su capacidad de negocio e innovación. Los activos de datos que tiene una organización pueden estar centrados en la propia relación de esa compañía con sus clientes que han permitido a la empresa para que utilice esa información en su negocio. El también conocido como data capital, en su sentido más amplio, está cobrando mayor relevancia a medida que se consideran como un bien tangible negociable o un valor negociable.

Dentro de los datos susceptibles de fines lucrativos, existen los datos personales, que refieren a aquellos que identifican o hacen identificable a una persona, y que tienen aún mayor valor económico que los datos comunes. Pero aún dentro de los datos personales, existen categorías que por su naturaleza, merecen una mayor protección dentro de su tratamiento, ya que podrían comprometer de sobre manera los derechos a la personalidad, tales como la autodeterminación informativa, y por lo tanto, deberían ser reconocidos y actualizados en las leyes de protección de datos, tales como los datos biométricos, datos médicos, datos genéticos, entre otros.

El problema en el caso de los datos personales y más específicamente los datos sensibles, siendo los datos biométricos en los que se centre esta investigación, es que, si bien los sistemas biométricos en general son seguros, las personas relacionadas con el tratamiento de datos pueden llegar a comprometer de sobre manera los derechos a la privacidad y la intimidad de la persona en alguna etapa del procesamiento, ya que al ser negociables y viables de lucro, sobre todo en manos de empresas, organizaciones, o entidades financieras, dejarían en estado de indefensión al titular de los mismos. Todo esto puede llegar a pasar por la falta de ética digital de los operadores del tratamiento, las brechas de seguridad en las que pudieran incurrir los particulares, la falta de cumplimiento de estándares de calidad, o que decir por la ausencia de especificaciones y lineamientos en las leyes de datos personales.

Se parte de la hipótesis de que la falta de reconocimiento de los datos biométricos como datos personales sensibles en México impide garantizar la

protección de los mismos dentro del territorio nacional, siendo la regulación de España y la Unión Europea los referentes para su consulta, estudio que puede asentar las bases para garantizar la protección de datos biométricos en México. Si bien su reconocimiento no es explícito en la ley mexicana, y al mismo tiempo no lo impide directamente ya que como tal existe un marco legal aplicable al tratamiento de datos por particulares, es una ley que no ha sido actualizada desde su promulgación y no ha incluido temas recientes de la época digital tal como los derechos digitales frente a los avances tecnológicos en Inteligencia Artificial o en las TIC, especificación de datos sensibles como los datos biométricos, categorías especiales de tratamiento, sanciones específicas por el tratamiento de datos especialmente sensibles, entre otros, por lo que se deduce que se ha encontrado parcialmente la hipótesis inicial planteada, ya que si bien de forma interpretativa los datos biométricos se equiparan a los datos sensibles, datos que si están reconocidos en México, su falta de especificación y actualización acorde a la época digital en que vivimos, y más aún en torno a los datos biométricos, deja una brecha de legalidad sobre los datos personales que debería subsanarse. La ley debe proveer lineamientos a las personas sujetas al tratamiento de datos que les permitan resolver la brecha de seguridad a la que puedan enfrentarse, delimitando claramente cuales datos deban ser especialmente protegidos, para así minimizar las posibles consecuencias derivadas de su tratamiento y evitar, de alguna forma, que vuelva a suceder en el futuro, tal como lo ha previsto el legislador europeo. Para analizar la hipótesis anterior, se decidió proceder con el esquema preliminar delimitado en el índice, partiendo desde la naturaleza e historia de la biometría, la conceptualización y características de los datos biométricos, generalidades de funcionamiento del sistema biométrico, el caso del tratamiento hecho por Entidades Financieras y particulares en general, hasta contemplar referencias de regulación en diversos países de Latinoamérica, siendo principalmente la comparativa de leyes de protección datos entre Europa, España y México.

Dicho estudio y comparación debe arrojar resultados que puedan servir de base para confrontar los nuevos desafíos en la era digital en México y se pueda plasmar en proyectos de reformas en materia de datos personales para actualizar el sistema normativo, específicamente en cuanto al tema de los datos biométricos, ya

que no solo en México es importante hacerlo, sino en todo el mundo, debido al fenómeno de la globalización tecnológica y digital en que vivimos.

En cuanto al contenido del capítulo I, se habla sobre la conceptualización de datos biométricos, sus antecedentes históricos más antiguos y recientes, así como algunas referencias, precisiones y formas de regulación de los mismos en algunos países de Latinoamérica, México y Europa. Por otro lado, en el capítulo II se analizan los sistemas jurídicos de los sujetos internacionales públicos comparados, para después proceder con el estudio pormenorizado de los ordenamientos legales sobre protección de datos de la Unión Europea, España y México, específicamente en torno al modo y la forma en como son regulados los tratamientos de los datos biométricos. Por lo que respecta al capítulo III, se procede con la estructuración de los resultados arrojados por el estudio comparativo entre el factor neutral y los datos biométricos derivados de las reglamentaciones legales de protección de datos estudiadas; también se menciona algunos efectos jurídicos que podrían surgir al momento que el legislador reconozca en *lato sensu* el hecho jurídico de la existencia de los datos biométricos; finalmente también se mencionan algunas consideraciones importantes que los particulares deberían tomar en cuenta como buenas prácticas al momento de ejercer el tratamiento de datos biométricos, tales como las evaluaciones de impacto como medio de amortiguamiento en el tratamiento, la transparencia en los procesos de decisiones automatizadas, así como la trascendencia de la privacidad por diseño y por defecto. Todo esto con la constante de que los operadores de sistemas informáticos mantengan en práctica la ética digital en el ejercicio de sus funciones.

Por lo anterior es que se utilizará el método analítico y deductivo para conocer la naturaleza y funcionamiento de los datos biométricos descritos en la doctrina, así como en algunas legislaciones de Latinoamérica; por otro lado a través del método sistemático se emprenderá un análisis de la legislación mexicana en relación con la protección de datos personales en posesión de particulares, en cuanto a los datos biométricos; y finalmente se utilizará el método comparativo para contrastar lo mencionado y regulado de los datos biométricos entre las legislaciones de la Unión Europea. España y México.

SIGLAS Y ABREVIATURAS

CPEUM	Constitución Política de los Estados Unidos Mexicanos
LFPDPPP	Ley Orgánica de Protección de Datos Personales en Posesión de Particulares
UE	Unión Europea
RGPD	Reglamento General de Protección de Datos
LOPDPGDD	Ley Orgánica de Protección de Datos y Garantías de los Derechos Digitales
LORTAD	Ley Orgánica De Regulación Del Tratamiento Automatizado De Los Datos De Carácter Personal
LOPD	Ley Orgánica de Protección de Datos
AEPD	Agencia Española de Protección de Datos
INAI	Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales.
CNBV	Comisión Nacional Bancaria y de Valores
FINTECH	Industria naciente en la que las empresas usan la tecnología para brindar servicios financieros

CAPÍTULO I. ANTECEDENTES, REFERENCIAS Y PRECISIONES DE LOS DATOS BIOMÉTRICOS EN LATINOAMÉRICA, MÉXICO Y EUROPA

SUMARIO: *1.1. Definición y antecedentes de la biometría 1.2. Generalidades del funcionamiento del sistema biométrico 1.3. Referencias en el sistema jurídico anglosajón y en Latinoamérica: Colombia, Argentina, Chile y México 1.4. Referencias en la legislación Europea Vigente y España 1.5. Conclusiones preliminares*

Es de suma importancia que los datos biométricos que son tratados por particulares, sean personas físicas o personas jurídicas de carácter privado, estén debidamente regulados y controlados por las legislaciones de protección de datos respectivas, siendo el caso particular de México que en su ordenamiento legal conocido como LFPDPPP ni siquiera haga mención a ello. Por supuesto que regula y ordena el tratamiento de los datos personales sensibles, que sobre éstos se consideran implícitos los datos biométricos, pero hace falta que se haga una especificación de los mismos, y por ello sea necesario realizar un bosquejo general de sus características, sus usos y sus riesgos, tomando como referencia algunos países que han logrado su regulación. Es por ello que se pretende realizar un estudio de los mismos para obtener un entendimiento general sobre su debida concepción.

1.1 Definición y antecedentes de la biometría

Previo a profundizar en las diferencias técnicas y legales de los datos biométricos, es necesario establecer un marco conceptual donde se identifiquen los conceptos de biometría, datos personales y datos sensibles, mismos que ayudan a delimitar el camino por el cual se emprenderá esta investigación. La motivación es dar a conocer el área de la biometría y su interrelación con la privacidad y la intimidad, derechos humanos protegidos en las leyes de diversos países por su interés en salvaguardar el derecho a la autodeterminación informativa

1.1.1 Conceptos afines

Para establecer un entendimiento general de la biometría, en primer punto es conveniente recurrir a la ontología misma de la palabra biometría, que deriva de palabras griegas: “*bios*” de vida y “*metron*” de medida. El Diccionario de la Real Academia Española[1] los define como el “estudio mensurativo o estadístico de los

[1] Concepto encontrado en el diccionario de la Real Academia Española a través de su buscador automático. *https://dle.rae.es*

fenómenos o procesos biológicos". Además, según el Diccionario de términos médicos, de la Real Academia Nacional de Medicina, menciona que éste también proviene del inglés *biometrics*, que se identifica como la "disciplina científica que se ocupa de los métodos automáticos para el reconocimiento único de un ser humano a partir de uno o más rasgos físicos o psíquicos concretos"[2]. Algunos ejemplos de técnicas biométricas con diversos fines son el reconocimiento de huella dactilar, de voz, de la forma de la mano, del iris, de la firma, el reconocimiento facial, entre otros. De igual forma se aplican principalmente como medidas de control de acceso físico, control de presencia y de acceso a información y recursos.

Asimismo, el Diccionario panhispánico del español jurídico, del Consejo General del Poder Judicial y de la Real Academia Española[3], define dato biométrico como "dato referido a las características físicas o fisiológicas o de conducta de una persona que permite su identificación única, como imagen facial o datos dactiloscópicos". El término, a su vez, aparece como sub lema de dato de carácter personal, identificándose cómo "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de otro tipo concerniente a personas físicas identificadas o identificables".

Por otro lado, de acuerdo a Vanessa Díaz[4] especialista en datos biométricos, la biometría es una técnica que a través de la estadística va a estudiar la diversidad de organismos y la población. Ésta se puede aplicar a diversas actividades sociales, pero también a diversas ciencias como la anatomía, biología, antropología, psicología, nuevas tecnologías de la información y comunicación, etcétera.

Ahora bien, surgiría la pregunta ¿En qué momento las características fisiológicas o de comportamiento del ser humano pasan a ser un dato biométrico? Para ello más adelante se dedica un subtema sobre el procesamiento de información en los sistemas biométricos, pero para responder en términos resumidos, se da al momento en que el usuario de un sistema biométrico, voluntariamente se dispone y se registra en el mismo, para ofrecer alguna característica física o de comportamiento

---

[2] Concepto encontrado en el Diccionario de términos médicos, de la Real Academia Nacional de Medicina *https://dtme.ranm.es/index.aspx*

[3] Concepto encontrado en el Diccionario panhispánico del español jurídico de la RAE https://dpej.rae.es

[4] Rodríguez, V. D. Sistemas biométricos en materia criminal: un estudio comparado. *Revista IUS, 7(31).* Enero-junio de 2013. *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100003*

de su cuerpo a través de algún sensor, que el sistema captura y lo procesa para crear una representación electrónica llamada modelo de referencia o *reference template*, debiéndose guardar en un archivo o base de datos, para proceder con su tratamiento y su proceso posterior tanto de identificación como de autenticación. Cabe mencionar que justamente este *biometric template* o datos que hacen identificable a una persona, es lo que se concebiría como datos biométricos dentro de un sistema biométrico.

En nuestro país, el organismo garante de acceso a la Información y Protección de Datos Personales, el INAI, emitió una Guía donde ofrece lineamientos claros sobre la naturaleza de éstos datos personales sensibles, mencionando en qué momento un dato biométrico se puede considerar dato personal: "Un dato biométrico será dato personal cuando de manera directa identifique a su titular, o bien, lo haga identificable a través de la biometría, pues sin la aplicación de este método serían desproporcionales los esfuerzos que se requerirían para reconocer a la persona."[5] A la par de este concepto, se trae a colación la definición de datos biométricos que ofrece esta guía, la cual refiere como "los datos biométricos son las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles"[6] Entre los datos biométricos que establecen las características físicas y fisiológicas de las personas se encuentran la huella digital, la retina, el iris, el reconocimiento facial, la geometría de la mano o de los dedos, la estructura de las venas de la mano, la forma de las orejas, pulsación cardíaca, la composición química del olor corporal y el patrón vascular, la piel o textura de la superficie dérmica, el ADN, neurodatos, entre otros. Todos estos datos biométricos son resguardados en plantillas biométricas que a su vez se encuentran en archivos o bases de datos, ya sea a cargo de particulares o de sujetos obligados, tal como lo refiere la legislación mexicana, siendo objeto de este estudio aquellos archivos o bases de datos que se encuentran en posesión de particulares, así como el tratamiento que brindan a los mismos.

Los datos biométricos, cumplen con cuatro características principales: son únicos e intransferibles, ya que la duplicidad no existe y por lo tanto nos distingue

---

[5] INAI, *"Guía para el tratamiento de datos biométricos",* marzo 2018, p. 19 *https://www.ssc.cdmx.gob.mx/storage/app/media/Transparencia/Documentos%20Transparencia/GuiaDatosBiometricos_Web_Links.pdf*

[6] Ibidem p. 9

como individuos; son permanentes, pues al ser fisiológicos, biológicos o conductuales, se mantienen a lo largo del tiempo en cada persona; son medibles ya que se manejan de forma cuantitativa; y también son considerados universales, toda vez que todos los seres humanos contamos con ellos.

Las características físicas y de comportamiento de una persona que pueden ser medidas a través de la biometría son únicas: es decir, no pueden ser robados, olvidados, duplicados o compartidos y por lo mismo, es de suma importancia el que estén debidamente salvaguardados donde se encuentren registrados, ya que una vez que dichas características están codificadas en sistemas biométricos, de acuerdo al tipo de dato que se esté utilizando y el fin por el que se esté disponiendo, puede existir algún tipo de fortalezas y debilidades en su manejo, acorde al fin que disponga el titular a terceras personas del tratamiento de estos, siempre dependiendo en gran medida de los estándares legales y de ciberseguridad necesarios para proteger los datos del titular. Cabe mencionar que existe un negocio importante en torno al tratamiento de datos personales a través de la mercantilización de los datos digitales, aspecto que no es menos importante ya que por su interés económico, existe el riesgo latente de violentar la privacidad de las personas titulares de los datos, si se incumplen los lineamientos legales que delimitan la protección de datos, así como las medidas de ciberseguridad básicas que deben preverse al momento de realizar el tratamiento de los mismos.

Los mecanismos de autenticación de acceso a sistemas informáticos se han vuelto cada vez más necesarios en ésta época en la que el desarrollo de nuevas tecnologías han evolucionado, y por lo tanto han detonado la democratización de la información, siendo la biometría uno de los métodos más actuales, pero paradójicamente de los más antiguos, tal como se verá en los referentes históricos.

1.1.2 Antecedentes históricos

Aunque pareciera que los datos biométricos son de época reciente, en realidad su estudio se remonta hace muchos años atrás. Específicamente el uso de las huellas digitales como marca de identidad personal tiene una larga historia. Hace 4.000 años, los babilonios ya las usaban para firmar contratos. Al menos desde el siglo XI a.C. ya

se conocía en China, de donde se cree que llegó a Persia con la dinastía de Tamerlán, en el siglo XIV[7]

De acuerdo al libro de Referencia de las huellas dactilares del departamento de Justicia de Estados Unidos, los chinos son la primera cultura que se conoce por haber utilizado impresiones de crestas de fricción como medio de identificación[8]. Siendo precisamente esas huellas digitales los referentes de los datos biométricos más antiguos como medios de identificación de una persona a través de su cuerpo físico. En general, el uso de crestas de fricción en piel como firma en China, India, Japón y posiblemente otros países antes del descubrimiento europeo, es muy bien conocido.

Existen referencias en la época del feudalismo donde se han identificado a trabajadores por diversas características físicas y morfológicas como cicatrices, color de los ojos, tamaño de la dentadura, lunares, etcétera. Esta clase de identificación se utilizaba en las zonas agrícolas. Los encargados de cuidar estos lugares debían identificar a cada uno de los propietarios cuando estos hicieran algún retiro de su mercancía, utilizando para esta tarea principios básicos de biometría como era identificarlos por sus rasgos físicos.

En el siglo XIX, estudiosos de la criminología tuvieron un gran interés cuando intentaron relacionar características físicas con tendencias criminales. En el año 1883, el francés Alphonse Bertillon[9], fue quien propuso un método de identificación de personas basado en el registro de las medidas de diversas partes del cuerpo, este método fracasó. Por otro lado, en los años 1822 a 1911, el antropólogo inglés Francis Galton[10], se dedicó a estudiar las características raciales hereditarias de las personas.

---

[7] Sánchez Arreseigor Juan José "las huellas dactilares, el arma perfecta de la policía para identificar personas" *National Geographic*, 2020, *https://historia.nationalgeographic.com.es/a/huellas-dactilares-arma-perfecta-de-policia-para-identificar-personas*

[8] Departamento de Justicia de los Estados Unidos, "El libro de referencia de las huellas dactilares", *Oficina de programas de Justicia*, Washinton DC, 2017, p. 5 *https://www.ncjrs.gov/pdffiles1/nij/249575.pdf*

[9] "Policía francés, hijo de Louis-Adolphe Bertillon (médico, antropólogo y estadístico al igual que el hermano de Alphonse, Jacques Bertillon, que también fue médico y estadístico). Se desempeñó como preceptor en Escocia y, a su regreso a Francia, trabajó para la policía de París. Investigador e impulsor de métodos de individualización antropológica". "Alphonse Bertillon", Biografías y Vidas, disponible en https://www.biografiasyvidas.com/biografia/b/bertillon.htm.

[10] Polímata, antropólogo, psicólogo y eugenista británico con un amplio espectro de intereses, fue el primero en aplicar métodos estadísticos para el estudio de las diferencias humanas y la herencia de la inteligencia, introdujo el uso de cuestionarios y encuestas para recoger datos sobre las comunidades

Dichas peculiaridades han sido consideradas para la identificación de los individuos. Esto propulsó un avance de diversos métodos de identificación. La idea de medir las características físicas de una persona, parecía efectiva y el desarrollo de la identificación de huellas digitales se convirtió en la metodología internacional para identificación utilizada por las fuerzas policiales de todo el mundo.

Con esta referencia y conocimiento, no es extraño que durante el siglo XX haya existido un gran interés en apoyarse de la tecnología informática para sistematizar y automatizar datos, disponiendo del poder de procesadores, sobre todo para la verificación de identidad por parte de individuos y organizaciones en cualquier ámbito de la sociedad. Robert Miller se dio cuenta de que las características distintivas de los tamaños y formas de las manos se podían utilizar para la identificación y patentó el primer dispositivo automatizado de geometría manual en el Instituto de Investigación de Stanford en 1971. En los últimos años, varios proyectos fueron comenzando a desarrollar la tecnología de la biometría, y uno de estos llevó a la creación de un lector de geometría de mano, siendo el primer medio para identificar a las personas por sus huellas dactilares. El éxito de su funcionamiento motivó a sus diseñadores a perfeccionar el concepto. Posteriormente, una compañía desarrolló un lector de geometría de mano, los cuales fueron dispuestos al mercado, siendo que a la postre se ha convertido en una de las bases de la industria biométrica.

A la par de otras metodologías biométricas como la verificación de huellas digitales que eran constantemente mejoradas, se llegó al punto de desarrollo tecnológico e informático donde los programas informáticos de reconocimiento biométrico, se convirtieron en equipos “confiables” y fácilmente manejables. En años recientes, se han creado sistemas de alta seguridad donde se realiza escaneo de iris, reconocimiento facial, reconocimiento corporal a través de la anatomía y fisiología del cuerpo, entre otros.

En la última década la industria de la biometría ha madurado considerablemente, gracias al desarrollo de un grupo de industrias especializadas que disponen de las tecnologías biométricas para mantener sistemas de seguridad para los teléfonos inteligentes, o de computadoras. Se dispone de una gran variedad de

humanas, que necesitaba para trabajos genealógicos y biográficos y para sus estudios antropométricos”, *Biografías y Vidas*, disponible en *https://www.biografiasyvidas.com/biografia/g/galton.htm*

equipos electrónicos capaces de identificar a las personas a partir de la información de alguna parte de su cuerpo, tales como físicas o de comportamiento. Incluso se pretende crear un sistema de identificación biométrica basado en el ADN y en los neurodatos.

Este tipo de tecnologías biométricas están creciendo y obteniendo una aceptación considerable, no sólo en aplicaciones de alta seguridad tales como bancos o áreas gubernamentales, sino también en centros de trabajo, centros de salud, control de derechohabientes del seguro social, plantas comerciales e industriales entre otros. Todo a la vez, ha provocado la imperiosa necesidad de regular el tratamiento de datos, sobre todo aquellos considerados como especialmente sensibles, tal como los datos biométricos, datos de salud o neurodatos.

Por otro lado existen ventajas al hacer uso de sistemas biométricos que reconocen las características especiales de las huellas digitales, por ejemplo, ya que se logra evitar fraudes en la banca, en el sistema de salud por suplantación de pacientes, controlar el acceso en el desplazamiento de trabajadores al interior de las empresas, etcétera; poco a poco se considera la necesidad de inutilizar las contraseñas, carnets, u otros medios de identificación vulnerables a ser jaqueados[11]. Los sistemas biométricos se han convertido en un medio mucho más rápido y seguro de identificación, y que a la par de su crecimiento, también se debería ir adoptando la tecnología en seguridad, tal como la cadena de bloques o *blockchain*[12], con el cual se pudiera contrarrestar de alguna forma los peligros de los malos usos de los expertos en el manejo de seguridad de los sistemas computacionales, y las consecuencias de efectos de la democratización de la información magnificados por el empleo cotidiano del internet y las bases de datos centralizadas.

Es por ello que de forma teórica, resulta de suma importancia el realizar un estudio sobre el devenir histórico en cuanto al uso, manejo y tratamiento de los datos biométricos para contextualizar y comprender de forma general su uso. Por otro lado

[11] La forma hackear es una semiadaptación poco recomendable a pesar de su extensión en el uso. El diccionario académico ya registra la adaptación jaquear, que es la que se recomienda usar en español y que se recoge en el DLE como jaquear. *https://www.rae.es/duda-linguistica/es-correcto-el-uso-de-hackear*

[12] Una base de datos distribuida y segura (gracias al cifrado) que se puede aplicar a todo tipo de transacciones que no tienen por qué ser necesariamente económicas. *https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda*

también es importante el comprender el sentido conceptual de los mismos, para que posteriormente se identifiquen las generalidades y formas de procesamiento de información biométrica, entendiendo a su vez cómo es que ésta información ya está regulada en su propia sistematización para su debido funcionamiento, pero que en conjunto con la ley y las buenas prácticas deberían garantizar el derecho a la autodeterminación informativa de los usuarios.

1.1.3 Marco conceptual de los datos biométricos

Para comprender las características de los datos biométricos, se debe desfragmentar el concepto de datos personales y abordar las medidas de seguridad que se disponen para el tratamiento de los mismos, siendo en tres puntos la forma en cómo se analizarán éstas características.

En primer punto, de acuerdo a la clasificación de los datos personales, a decir de Vanessa Díaz, se identifican los siguientes:

1. Datos identificativos
2. Datos electrónicos
3. Datos laborales
4. Datos patrimoniales
5. Datos sobre procedimientos judiciales y/o administrativos
6. Datos académicos
7. Datos de tránsito y movimientos migratorios
8. Datos sobre la salud
9. Datos personales de naturaleza pública
10. Datos sensibles
11. Datos biométricos
12. Neurodatos

Los datos biométricos se pueden clasificar tradicionalmente según dos formas: por sus propias características como los rasgos, ya sean físicos, fisiológicos, morfológicos o de comportamiento, o bien de acuerdo al *software* utilizado para su almacenamiento y autenticación ya sea a través de señales o tipos de sensores.

En segundo punto, la ciberseguridad es el área pertinente que analiza los criterios de seguridad con que se rige un sistema, y por lo tanto para garantizar la

seguridad de los datos debe comprender claramente la naturaleza y el tipo de los mismos, con el objeto de identificar sus fortalezas y debilidades, dentro del tratamiento hecho ya sea por personas físicas, jurídicas o a través de sistemas automatizados. Por lo que es pertinente remitirse a las medidas que se toman para su protección una vez que se encuentran en los sistemas, así como la identificación o clasificación de los datos personales, a saber:

Dentro de las medidas de seguridad que se toman para la protección de datos una vez digitalizadas, son las siguientes:

1. Identificar los datos personales que la doctrina conoce así como su tipo
2. Delimitar el nivel de datos en cuanto a su categorización
3. Elaboración de documentos de seguridad y privacidad para proteger esos datos personales
4. La implementación de las medidas de seguridad de acuerdo al nivel de los datos

La tipología de los datos biométricos se subdivide de acuerdo a las características fisiológicas, morfológicas, biológicas como el ADN o neurológicas como los neurodatos. Por un lado, dentro de las características fisiológicas se encuentran: la composición química del cuerpo, el iris y la retina, huellas dactilares, impresiones de la palma de la mano o pies, la geometría de la mano, el rostro y los poros de la piel, las papilas gustativas, la estatura, la temperatura, entre otros. Por otro lado, dentro de las características morfológicas, existe la escritura, la firma, la voz, la forma de caminar, de teclear, etcétera.

Cabe resaltar que los datos biométricos cuando son compartidos entre sistemas con el objetivo de identificar y/o verificar a los individuos, es el momento en que las leyes de protección de datos los deberían categorizar como información personal sensible, ya que hay muchos datos manejados que pueden ayudar precisamente a la identificación, y al conjunto de datos personales que tienen como fin el identificar o autentificar a una persona se categoriza precisamente como datos sensibles.

En tercer punto, es importante mencionar las áreas donde se da la implementación de los sistemas biométricos para la identificación y autenticación de las personas, siendo claramente en los archivos o bases de datos, tales como las bases de datos de ADN con fines de identificar desaparecidos, las de recién nacidos,

de filiación, bases de datos criminales, bases de datos migratorias, poblacionales, clínicas, electorales, de licencias, entre otras.

1.2 Generalidades del funcionamiento del sistema biométrico

Para comprender de forma mucho más amplia las características de los datos biométricos, es necesario también profundizarlo en su sentido práctico. Los sistemas que utilizan datos biométricos para la identificación de individuos realizan esta tarea por medio de un proceso de identificación o de verificación, consistentes en la comparación entre muestras biométricas, una recolectada previamente y una posterior. Es importante conocer su funcionamiento para familiarizarse con el largo proceso informático que conlleva su recolección y tratamiento, ya sea por parte de los sujetos obligados o los particulares, así como los entes económicos o entidades financieras, ya que comprenderlo, nos permite un entendimiento mucho más integral y completo de la naturaleza de los datos biométricos.

Es importante mencionar que las características biométricas que recogen los *software* de autenticación, tienen en común lo siguiente:

1. Universales: Son las características básicas que integran a un individuo[13]
2. Registrables: Características particulares de cada individuo, que pueden ser almacenadas en una base de datos y que requieren el consentimiento expreso del titular para su tratamiento[14]
3. Únicas: Son las características que hacen diferente a cada individuo[15]
4. Medibles: Dato biométrico registrado y almacenado, que puede ser medible en un futuro[16]

Éstas características biométricas demuestran lo eficaces que son para identificar a una persona, siendo utilizado mayormente como medio de autenticación de los usuarios para que de esta forma se proteja a los titulares.

---

[13] Centro Criptológico Nacional, "Glosario AAA, Authentication, Authorization and Accounting, Cryptex-Seguridad Informática", *España Blogger.com*, 4 de abril de 2008 disponible en *http://seguridad-informacion.blogspot.com/2008/04/glosarioaaa-authentication.html.*

[14] *Ídem*

[15] *ídem*

[16] *ídem*

1.2.1 El procesamiento de información

Desde un punto de vista de sistemas informáticos, los datos biométricos son una medida digital de información privada y personal que necesita de un *software* potente que, haciendo uso de diversos campos de la informática para sintetizar la información, tal como el escáner, la Inteligencia Artificial, o algoritmos matemáticos complejos, en conjunto funcionen dentro de un sistema biométrico para que pueda medir, codificar, comparar, almacenar, transmitir y reconocer las propiedades físicas, fisiológicas, de comportamiento o rasgos característicos de la personalidad de los usuarios, a través de sensores biométricos o sistemas de captación, que básicamente se divide en cuatro, a saber: sensores ópticos, sensores capacitivos, sensores termoeléctricos y micrófonos ópticos unidireccionales. Cada uno de estos medios, dan inicio al procesamiento de modelos de referencia (*reference template*), que a través del sistema biométrico genérico de información, cubre desde la recolección de datos, la transmisión, el procesado de señal, la de decisión, hasta el almacenamiento de datos. Cabe mencionar que los datos que se envían y se tratan dentro de todo este procesamiento de información del sistema biométrico, lo es una representación electrónica del usuario que comprueba la identidad del usuario mismo, o tal como lo menciona el INAI en la guía mencionada, conocidos como plantillas biométricas. Se puede deducir que la criptografía prácticamente es un método secundario dentro de este gran sistema, pero que resulta de suma importancia en el mismo, ya que se encarga de salvaguardar a través del cifrado la información trabajada.

Una vez delimitado el procesamiento de información, tal como se ha mencionado anteriormente, es necesario también comprender la forma en cómo son estandarizados los procesamientos de información de los datos biométricos para tener un entendimiento mucho más integral del largo proceso de tratamiento de datos.

1.2.2 El caso de los estándares aplicables al procesamiento de información

En entornos globalizados, es necesario que los estándares sean interoperables, sino no existiría la información biométrica en sí. Es decir, no sirve de nada tener un sistema si no se puede compartir. Es por esto que las organizaciones y corporaciones internacionales han desarrollado diferentes estándares o protocolos de interoperabilidad, que de acuerdo a Vanessa Díaz, no es otra cosa que permitir la lectura del almacenamiento o tratamiento de la información. Los estándares han sido

creados para establecer los lineamientos básicos para el procesamiento de información, formados por organizaciones de estándares formales e informales. Es imperioso mencionar que las distintas organizaciones quienes están activamente involucradas en el desarrollo de los estándares y su adopción son algunas de las siguientes:

- Organización de Estándares Internacionales (ISO)
- Instituto Nacional de Estándares y Tecnología (NIST)
- Comité Técnico Conjunto 1 (JTC 1) /Subcomité 37 (SC 37)
- Organización para el progreso de Estándares de Información Estructurados (OASIS)
- Comité Internacional para Estándares de la Tecnología de la Información (INCITS) M1

Esto surge como una iniciativa por parte de los particulares de mantener estándares de compartición de datos entre ellos. Gracias a los avances tecnológicos se han creado bases de datos inagotables que contienen datos biométricos de distintas personas, provocando que diversas instituciones colaboren mundialmente para compartir información e intercambiar datos en forma mucho más rápida y fácil. Es por ello que existen los estándares en comunicación y protocolos para el intercambio de datos. A continuación se presentan algunos estándares que resaltan en el tema:

- "Estándar ANSI X.9.84: creado en 2001, por la ANSI (*American National Standards Institute*) y actualizado en 2003, define las condiciones de los sistemas biométricos para la industria de servicios financieros haciendo referencia a la transmisión y almacenamiento seguro de información biométrica, y a la seguridad del hardware asociado.
- Estándar ANSI / INCITS 358: creado en 2002 por ANSI y *BioApi Consortium*, presenta una interfaz de programación de aplicación que garantiza que los productos y sistemas que cumplen este estándar son interoperables entre sí.
- Estándar NISTIR 6529: también conocido como CBEFF (*Common Biometric Exchange File Format*) es un estándar creado en 1999 por NIST y *Biometrics* Consortium que propone un formato estandarizado (estructura lógica de archivos de datos) para el intercambio de información biométrica.

- Estándar ANSI 378: creado en 2004 por la ANSI, establece criterios para representar e intercambiar la información de las huellas dactilares a través del uso de minucias. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de identidad e identificación, empleando información biométrica proveniente de otros sistemas.
- Estándar ISO 19794-2: creado en 2005 por la ISO/IEC con propósitos similares a la norma ANSI 378, respecto a la que guarda mucha similitud.
- Estándar PIV-071006: creado en 2006 por el NIST y el FBI en el contexto de la norma FIPS 201 del gobierno de EE.UU. establece los criterios de calidad de imagen que deben cumplir los lectores de huellas dactilares para poder ser usados en procesos de verificación de identidad en agencias federales".[17]

Los estándares de calidad que se siguen en las empresas, industrias y corporaciones permiten comprender la forma en cómo es regulado el manejo de la información biométrica por diversas personas físicas o jurídicas, siendo un aspecto importante para conocer de forma práctica y teórica los datos biométricos. La importancia de atender los estándares de calidad en este sector radica principalmente en ofrecer los servicios adecuadamente, en donde, principalmente, se intentan prevenir riesgos a futuro. Por supuesto, todo *software* puede tener fallos que terminen siendo responsables de grandes pérdidas de dinero para la empresa, además de involucrarlas en responsabilidades legales por las brechas de seguridad en el tratamiento de datos. Por lo tanto, mientras más tarde se detecten los defectos o errores de los sistemas, mayores pueden ser las consecuencias. Es por ello que, además de atender los lineamientos legales para el tratamiento de datos, se deben considerar los estándares aplicables al procesamiento de información biométrica, acompañado de buenas prácticas y la privacidad por diseño y por defecto.

Una vez identificados ciertos antecedentes, conceptos y generalidades de funcionamiento y procesamiento de información de los datos biométricos, se pretende analizar brevemente diversas formas de regulación de tecnologías biométricas, en el contexto específico de las referencias legales existentes en ciertos países. Este análisis nos permitiría identificar las propensiones legales en el tema, para así plantear algunas conclusiones y recomendaciones de cara a la eventual actualización

[17] "Biometría", Wikipedia, disponible en *https://es.wikipedia.org/wiki/Biometr%C3%ADa*.

de la regulación en la materia del país mexicano. Posteriormente, en el capítulo II se procederá a realizar el estudio de derecho comparado con base en la metodología de la macrocomparación, entre la Unión Europea, España y México.

1.3 Referencias en el sistema jurídico anglosajón y en Latinoamérica

El objetivo de remitirse a ciertos países de los dos sistemas jurídicos más conocidos en occidente como lo es el anglosajón y el romano-germánico, es identificar las conceptualizaciones hechas sobre privacidad y datos personales, específicamente lo relacionado con los datos biométricos, así como identificar las instituciones jurídicas creadas y el contenido de los cuerpos normativos que las crean. El conocer los derechos y obligaciones que regulan los países de diferentes sistemas jurídicos en torno a los datos personales, son importantes para compendiar derechos y contrastar su análisis y estudio, ya que esto no solo es para aquellos estudiosos de la ley, sino para todas las personas que finalmente están sujetas al orden jurídico, situación que cobra gran relevancia, pues solo así es cómo se pueden efectivizar los derechos del orden normativo, en tanto las personas conozcan y hagan efectivos los procedimientos para su aplicación, así como el uso de las instituciones que comprenden su propio sistema jurídico.

Por un lado, se hace alusión a ciertos países del sistema jurídico anglosajón debido a que es dentro de esa tradición donde se conceptualiza inicialmente lo que es la privacidad, siendo un referente importantísimo en el marco de los datos personales. Por otro lado, se ha tomado como referencia ciertos países de Latinoamérica tales como Colombia, Argentina y Chile debido a su gran avance dentro de la positivización de los derechos digitales en el sistema jurídico romano-germánico, específicamente en relación con la regulación del tratamiento de los datos personales, que si bien no son los países de quienes se toman modelos de referencia sobre derecho comparado, su conocimiento permite enriquecer la conceptualización de la protección de datos biométricos en México, debido a que en este caso, sus sistemas jurídicos son similares al de nuestro país, y por lo tanto se puede tener un amplio espectro de compresión y aplicación en tierras latinas frente a la influencia europea, asiática y americana, quienes son sin duda alguna las grandes potencias mundiales en la época digital.

1.3.1 El caso referencial de la *right to privacy* del sistema jurídico anglosajón

La privacidad no era una palabra castellana sino hasta hace apenas algunos años. De hecho tiene raíces anglosajonas conocida ampliamente bajo el concepto de la *privacy*, que básicamente se traduce al español como "intimidad", pero se ha castellanizado esta palabra por un motivo, el cual es diferenciarla fundamentalmente de lo que es en sí mismo la intimidad[18]. Es importante identificar que existen dos sistemas distintos para concebir la privacidad, por un lado la *privacy* de Estados Unidos de Norteamérica, y por el otro la privacidad en Europa y países del sistema jurídico romano-germánico.

En su aspecto teórico, la doctrina de los países del sistema jurídico anglosajón lo identifican como *right to privacy,* donde lo definen como "el derecho a gozar de la vida, o sea, del derecho a estar solo *(right to be alone[19])"* En aquellos países del *common law* tienen bien definido los conceptos de lo que es público y de lo que es privado, y que de acuerdo a Matteucci, "es el antagonismo que existe entre la esfera pública y esfera privada"[20], una dialéctica que establece los principios del derecho a la intimidad, la vida privada, derecho a la identidad y a la personalidad, y que de acuerdo a la tradición jurídica anglosajona, el polo de la dicotomía público-privado es el propio individuo, aspectos que en la tradición jurídica romanista encuentran serias dificultades al momento de explicar el concepto de *privacy.* Este concepto se convierte en una barrera o límite para el Estado y cualquier otro ente jurídico porque lo público se define y fundamenta a partir de lo privado[21]. De acuerdo a este entendimiento, la esfera privada pasa a convertirse en el mundo fenomenológico, como la base del desarrollo de la conciencia, el medio para conseguir la autorrealización del ser, dentro del plano donde se forma la progresión de valores éticos del ser humano, y donde éste crea, forma y finalmente manifiesta su personalidad para hacerle frente al mundo objetivo.

---

[18] Victor Salgado, Webinar "GDPR: El nuevo Reglamento Europeo de Protección de Datos" *https://www.youtube.com/watch?v=DSocLk5Mi8Q&t=2589s*

[19] Warren, S.D. Brandeis, LD. "The right to privacy"*,* en *Harvard Law Review*, 1980. Vol. IV, n° 5, p. 193

[20] Matteucci, N., "Introduzione público e privato" en *Privacy e banche dei dati (aspetti giuridicci e sociali),* AA. VV. Bolonia, 1981, p. 21

[21] Morales, P.F. "La tutela penal de la intimidad: privacy e informática" *ediciones Destino*, colección nuevo derecho, p. 17

El aspecto teórico de la *privacy* de esta tradición jurídica es robusto y fundamental, pero curiosamente se regula de una manera distinta a Europa y países del sistema romano-germánico, ya que en Estados Unidos de Norteamérica no se reconoce como un derecho constitucional ni se menciona en ninguna parte de su contenido. La *privacy* ha sido definida por la doctrina y la jurisprudencia, incluso mucho antes que en Europa a finales en el siglo XIX, siendo hasta después que ciertos estados como Illinois, Texas y Washington tienen su propia normatividad. La forma en cómo se regula los datos personales son a través de las conocidas como "políticas de privacidad", que quedan a cargo de cada entidad jurídica o empresa el establecer la forma en cómo brindará tratamiento a los datos, adecuándose a los estándares de calidad anteriormente mencionados, donde se incluya y se informe al titular de lo que hacen con sus datos a través de esas políticas. Una vez que el interesado ha aceptado esas políticas de privacidad, se podría decir que el dueño de los datos personales lo es la propia organización o empresa.

Claro está que en México no contamos con el mismo sistema jurídico, pero el concepto de *privacy* de Estados Unidos justifica plenamente el reconocimiento a la vida privada, derecho ya reconocido en nuestra constitución[22] y por lo tanto en nuestro país refuerza doctrinal y fundamentalmente el derecho a la libre autodeterminación informativa. En Australia por ejemplo, según *Australian Privacy Principles* considera que la información biométrica es información confidencial, además que el objeto de estos principios es garantizar que las entidades gestionen la información personal de forma abierta y transparente.[23] O en Estados Unidos de Norteamérica, la primera acta de protección de datos biométricos fue la *Illinois Biometric Information Privacy* Act (BIPA) que desde 1998, es la primera regulación de aquel país[24]. El mismo derecho al olvido que reconocen algunas empresas internacionales como Google o Meta provienen de la reglamentación del derecho interno de algunos países de la tradición jurídica anglosajona, quienes han introducido globalmente el concepto de "políticas

[22] Artículo 6o.- La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado. p. 12 *https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf*

[23] Australian Government "Read the Australian Privacy Principles" *https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles*

[24] Natalie A. Prescott, The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020 National Law Review, *https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020*

de privacidad” las cuales, una vez aceptadas por el titular o el interesado, no existe mayor detenimiento por parte del estado para con las empresas, ya que de alguna forma, y salvo algunas excepciones, en Estados Unidos y algunos otros países anglosajones está liberalizado el tratamiento de los datos personales.

De acuerdo a los puntos doctrinales y legales de los países vistos del sistema jurídico anglosajón, se llega a comprender que, al haber aportado los cimientos de la *privacy*, se pueda tomar como referencia doctrinal al momento de delimitar el polo de la dicotomía público-privado dentro del propio individuo. Pero además de estas referencias doctrinales, en el sistema jurídico romano-germánico de nuestro país se podría esperar que no solamente quede a expensas de las políticas de privacidad de los particulares, sino que se reconozca la vida privada como un derecho humano, y por lo tanto se vea obligado a crear un *habeas data* para satisfacer su garantía, tal como se podrá analizar en algunos países latinoamericanos.

1.3.2 Colombia

En cuanto a éste país, se ha decido estudiar sus características generales de protección de datos, debido a los avances que a nivel Latinoamérica lleva a cabo hasta la actualidad. Es bien conocido que en el artículo 15 de la Constitución de Colombia de 1991, donde se tutela el derecho fundamental de *habeas data,* refiere a la protección de datos, que en los últimos años ha tomado fuerza con la implementación de nuevas normas que tienen como fin salvaguardar los derechos y deberes fundamentales, así como los procedimientos y recursos para la protección de los mismos.[25] Se dio la Ley 1266 de 2008 como norma especial, con la finalidad de proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones como recolección, almacenamiento, uso y tratamiento por parte de entidades de naturaleza pública y privada. Las personas jurídicas que manejan mecanismos técnicos para la identificación biométrica de las personas físicas, están obligadas, conforme a lo dispuesto por la Ley 1581 de 2012, a solicitar la debida autorización por parte del titular de los mismos.

En Colombia la biometría inició como un método de identificación de personas, para verificar que un individuo es quien dice ser. A medida que esta tecnología se

[25] Colombia, Corte Constitucional, Sentencia C-748 de 6 de octubre de 2011 *https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm*

volvió más popular, fue utilizada por diversas empresas, las que han hecho uso de diversas herramientas biométricas, que incluyen el verificar la identidad de una persona, desde las más básicas como administrar el acceso a sus instalaciones, o más complejas como transacciones bancarias, acceso a cajas de seguridad, ingreso a redes de Internet, trámites ante el gobierno, entre muchos otros. Actualmente existe la Registraduría Nacional del Estado Civil, quien efectúa el proceso pertinente para lograr la firma de convenios que permitan por primera vez acceder al Sistema de Identificación Automatizada de Huellas Dactilares, y poder realizar autenticación biométrica de ciudadanos.[26]

El objetivo de citar la forma en cómo se regulan los datos biométricos en Colombia es debido a la importancia de ser tomados en cuenta en México, al momento de especificar la forma en cómo se reconocerían y se regularían en el área específica de la definición de datos sensibles de la LFPDPPP, así como la forma en cómo se salvaguarda la información en el Sistema de Identificación Automatizada de Huellas Dactilares de Colombia, pudiéndose realizar una institución especializada en materia de datos personales en México en algún momento, ya que como es bien sabido, el INAI ejerce dos funciones, del acceso a la información, y protección de datos personales, aspectos que deberían ser abordados por agencias especializadas tal como se hace en Colombia o algunos otros países.

1.3.3 Argentina

En éste país, existe una reconocida asociación que ofrece en medios digitales información con respecto a la definición y naturaleza de los datos biométricos en el idioma español llamada Asociación por los Derechos Civiles de Argentina, fundada en 1995, que trabaja en la defensa y promoción de los derechos civiles y humanos en Argentina y América Latina, del cual se consultó el libro digital denominado como: “la identidad que no podemos cambiar: cómo la biometría afecta nuestros derechos humanos.” Informe hecho por Leandro Ucciferri en abril de 2017, documento en PDF que se tomó en cuenta para la investigación conceptual de los datos biométricos, en donde se define como: “La biometría es el proceso por el cual se busca reconocer, autenticar e identificar a una persona, en base a sus características físicas o de

[26] Registraduría Nacional del Estado Civil, *“Identificación biométrica: cada vez con más usos en la vida cotidiana”* Gobierno de Colombia. *https://www.registraduria.gov.co/Identificacion-biometrica-cada-vez.html*

comportamiento. Generalmente se la clasifica en tres categorías de características: biológicas, morfológicas y de comportamiento."[27]

En el 2011, la presidencia emitió el decreto 1766/2011 donde, a través del ministerio de seguridad se creó el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) que tiene por objeto prestar un servicio centralizado de información respecto de los registros patronímicos y biológicos individuales, a los fines de contribuir a la comprobación idónea y oportuna en materia de identificación de personas y rastros, en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad.[28] Cabe resaltar que SIBIOS se muestra como una referencia de lo que se debería o no se debería hacer en nuestro país, ya que ha sido muy objetado por la materia en seguridad que se ve envuelto.

Se toma en consideración esta asociación argentina debido a los aportes que han hecho en Latinoamérica en relación con los derechos digitales y la regulación de los datos biométricos, que puede servir como guía al momento de regularlos en México, específicamente en lo que se debería hacer o no se debería hacer sobre la creación de alguna institución de datos biométricos con fines de seguridad, tal como la del ministerio de seguridad que creó el SIBIOS y el fin que se le ha dado en torno a la misma.

1.3.4 Chile

Existen importantes documentos de la organización chilena independiente llamada Derechos Digitales América Latina, fundada en 2005, la cual tiene como objetivo fundamental el desarrollo, la defensa y la promoción de los derechos humanos en el entorno digital. Continuamente realizan publicaciones de artículos, publicaciones y documentos digitales en PDF, en relación con los temas de libertad de expresión, derechos de autor y privacidad, siendo precisamente en esta última la que tenga relación con los datos biométricos. Un buen referente de éstos, se encuentra en el libro digital de 2018 llamado "El cuerpo como dato" de Marianne Díaz, donde se habla, de entre otros temas, sobre la naturaleza jurídica del dato biométrico,

[27] Ucciferri, "la identidad que no podemos cambiar: cómo la biometría afecta nuestros derechos humanos", 2017 p. 5 *https://adc.org.ar/informes/la-identidad-que-no-podemos-cambiar-biometria-sibios/*

[28] Ministerio de Justicia y Derechos Humanos, *"Decreto 1766/2011",* Presidencia de la Nación *http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm*

las tecnologías biométricas y los riesgos que conlleva, así como el rol de los actores privados, entre otros. Precisamente en cuanto a la biometría, se dice que "funciona sobre la base del supuesto de que ciertos rasgos físicos o conductuales son únicos al individuo, ya sea por sí solos o en combinación con otros; y a partir de estos datos, transformados en una plantilla (la representación digital de este rasgo), se crea la posibilidad de la identificación o la autentificación del individuo"[29]

Aunque en la Ley Chilena, los datos biométricos no se encuentran aún regulados expresamente, existe un ordenamiento jurídico que delimita la protección de datos personales: la ley 19.628 sobre la protección de la vida privada, la cual regula las condiciones y requisitos que se deben cumplir al recolectar, procesar y tratar los datos personales de un individuo. Existe una regla general donde solamente se pueden tratar los datos de un individuo con su consentimiento y, al momento de recolectarse los datos, estos solo pueden ser utilizados para el objetivo del cual fueron recolectados. Esto por supuesto que puede ser aplicado en el manejo de datos biométricos, pero sigue quedando pendiente de inclusión en la ley chilena en comento.

Por otro lado, Chile es pionero en reconocer constitucionalmente los neuroderechos[30], ya que en su proyecto de ley prohíbe el uso de neurotecnología en ciertos supuestos[31], tal como pacientes que llegan inconscientes a los hospitales o personas que no tienen la capacidad de comunicarse. En el fondo, esta ley apunta a establecer un nuevo derecho humano que garantice la integridad física, psicológica y por supuesto social y espiritual de las personas. A decir de la UNESCO "La adopción de tal arsenal jurídico puede parecer prematura a la vista del desarrollo de las neurotecnologías, todavía limitadas en su capacidad de actuar sobre el cerebro humano. Pero los expertos ya han dado la voz de alarma e insisten en la capacidad

[29] Marianne Diaz, "el cuerpo como dato", *Derechos Digitales & Ford foundation*, Junio 2018 p. 6 *https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf*

[30] el neuroderecho se ocupa de la regulación jurídica de la investigación y práctica neurocientífica; el papel de las neurociencias en el razonamiento probatorio; y el estudio de la actividad neurocognitiva de los operadores jurídicos. Podemos caracterizar los Neuroderechos en cuatro áreas: A) Identidad, libertad y agencia personal. B) Privacidad y consentimiento. C) Mejoramiento. D) Equidad e imparcialidad. p. 66 *http://revistaderecho.posgrado.unam.mx/index.php/rpd/article/view/179/356*

[31] Chile, pionero en la protección de los "neuroderechos" *https://es.unesco.org/courier/2022-1/chile-pionero-proteccion-neuroderechos*

de empezar a legislar la generalización de actividades intrusivas, mientras los progresos en el ámbito de las neurotecnologías no dejan de acelerarse."[32]

Sin duda alguna, Chile es un gran referente en la protección de los derechos digitales, específicamente en el área de la protección de datos personales, debido al gran estudio que por tantos años han realizado en torno a estos derechos, y que ha influenciado a nivel Latinoamérica para delimitar los derechos digitales, esperando que nuestro país tome cartas en el asunto y actualice la ley en torno a los mismos.

1.3.5 México

En el Artículo 6° constitucional se establece el derecho a la libertad de expresión y la privacidad, donde se definen los límites a estos derechos. Otorga el derecho a acceder a la información pública, y establece el proceso por el cual el Estado Mexicano está obligado a garantizar el acceso a las Tecnologías de la Información y Comunicación, así como el derecho a la privacidad y protección de datos personales, siendo la referencia constitucional al reconocimiento del *habeas data* en nuestro país. Aunque México no cuenta con un mecanismo jurídico especializado para garantizar la protección de datos personales, se cuenta con procesos legales tal como el recurso de revisión ante los Órganos Garantes, o en cuanto al control constitucional, el juicio de Amparo. Cabe mencionar que el artículo 16° de la constitución reconoce los derechos ARCO anteriormente mencionados, como derechos de las personas para hacer valer su derecho a la libre autodeterminación informativa.

Los datos personales son regulados en dos formas a través de dos leyes complementarias: aquellos manejados por sujetos obligados, y aquellos manejados por los particulares, sean personas físicas o morales. La LGPDPPSO y la LFPDPPP respectivamente.

Previo a esta reforma, el derecho de protección de datos personales se encontraba inmerso en la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* del año 2002. Con el objetivo de la promulgación de una ley específica en materia de protección de datos personales, después de ciertas iniciativas con diferentes matices que se dieron entre 2001 al 2009, no fue sino hasta

[32] Ídem

el año 2010 cuando se aprobó y se promulgó la LFPDPPP, con objeto de regular el derecho a la autodeterminación informativa[33], la cual tomó como base las reformas constitucionales del año 2009 a la que se hizo mención anteriormente, siendo precisamente esta ley la que se tomará de base para la colisión de contenido con la Ley Europea y la Ley Española respectivamente.

Ahora bien, el INAI, como se mencionó inicialmente, ha emitido la Guía para el Tratamiento de Datos Biométricos, donde se establece los lineamientos básicos sobre su manejo, pero que no es propiamente una ley, siendo precisamente el trabajo legislativo pendiente por realizar en esta materia.

Los datos biométricos utilizados por sistemas informáticos pueden ser catalogados, por interpretación axiológica, en la regulación mexicana de ambos códigos, como datos sensibles, debiendo cumplir al menos dos condiciones para identificar un dato personal:

1. Que se refiere a una persona física, y
2. Que identifica o hace identificable a su titular.

De tal suerte que los datos biométricos, al ser características o rasgos atribuibles a una persona y que son medibles, cumplen con el primer requisito para ser considerados como un dato personal. Sin embargo, para el segundo requisito se debe distinguir claramente, ya que hay algunos datos biométricos que por sí mismos identifican a una persona; sin embargo, existen otros que requieren de un procesamiento o de información suplementario para poder reconocer al titular.

De acuerdo a la Guía en comento, se menciona que el responsable del manejo de datos personales o datos sensibles, sólo podrá utilizarlos para las finalidades declaradas en el aviso de privacidad, siendo vedado el condicionar el tratamiento principal por uno secundario. Al realizarse transferencias de datos personales, los responsables deben informar a los titulares, e igualmente recabar el consentimiento

[33] El Derecho a la autodeterminación informativa hace referencia a la prerrogativa que todo individuo tiene frente a cualquier ente público o privado, por la cual nadie debe introducirse, sin autorización expresa (de él mismo o por mandato de ley o judicial), en aquellos aspectos que no son públicos –sino de su vida personal, familiar, documentos, correspondencia y domicilio–, para conocerlos, conservarlos, procesarlos y/o transmitirlos, independientemente de que dicha acción le cause o no, algún daño o molestia. p. 8 *https://www.tfja.gob.mx/investigaciones/historico/pdf/elderechoalaautodeterminacion.pdf*

para ello en caso de que el tipo de datos así lo requiera, obligándose el encargado al que se le haga la entrega de los datos a garantizar igualmente los principios a los que se encuentra obligado el responsable. Asimismo, el responsable debe garantizar el efectivo ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición ARCO, a fin de que sean operantes.

Un aspecto que genera importantes dudas para los responsables que recaban y tratan datos personales, es la relativa a la "sensibilidad" o categorías especiales de datos personales, y por lo tanto el tipo de tratamiento que debería implicar el manejar los datos biométricos, ya que el mismo INAI lo reconoce, al declarar:

> "Si bien los datos biométricos no están mencionados de manera expresa en el listado de datos personales sensibles que se incluyen en ambas leyes14, ello no implica que no se puedan considerar como tales bajo ciertas circunstancias. Para determinar tal característica, se requiere atender las condiciones del caso concreto, a fin de analizar si los datos biométricos en cuestión actualizan alguno de los siguientes tres supuestos que prevén la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares para considerar un dato personal como sensible:
>
> a) Que se refieran a la esfera más íntima de su titular;
> b) Que su utilización indebida pueda dar origen a discriminación, o
> c) Que su uso ilegítimo conlleve un grave riesgo para su titular."[34]

Es decir, los datos biométricos no se mencionan en la ley, y lo que es igual, no se especifica que éstos pudieran ser de alguna categoría especial y todo lo que eso implica. Si bien la ley reconoce algunos datos sensibles, ni siquiera hace mención de éstos. Pero al mismo tiempo no significa que no estén protegidos por la ley mexicana, ya que al momento de declarar que se ha violentado la privacidad por el tratamiento de datos biométricos ante el INAI, éste inmediatamente actúa e interpreta que dentro de la variedad de datos sensibles, los biométricos son parte de esta gama, postulándose en los casos en que el dato sensible del iris por ejemplo, pueda llegar a aportar información sobre el estado de salud de su titular, o el caso del tratamiento de una huella digital en aquellos casos en que su uso indebido puede permitir el acceso a información privilegiada que pudiera poner en riesgo la seguridad o el patrimonio del titular de los datos. Pero esta delimitación no puede quedarse a simple interpretación axiológica de los particulares o hasta el momento en que el Órgano

[34] INAI, *"Guía para el tratamiento de datos biométricos",* marzo 2018, p. 19 *https://www.ssc.cdmx.gob.mx/storage/app/media/Transparencia/Documentos%20Transparencia/GuiaDatosBiometricos_Web_Links.pdf*

Garante lo explique, sino que debe establecerse claramente en la ley respectiva, sobre todo delimitando la categoría especial de tratamiento de este tipo de datos, estableciendo a su vez la sanción específica que sea pertinente.

Es importante que a la brevedad posible sean regulados estos puntos de una manera mucho más específica, ya que el tratamiento de los datos biométricos por parte de particulares debería estar claramente delimitado, y no quede a interpretación que los datos biométricos son especialmente sensibles y merecen un tratamiento especial. Es por ello que el objetivo de realizar esta tesis sea para establecer algún precedente en la investigación de estos tipos de datos sensibles en México y la importancia de su especificación.

1.3.5.1 Manejo de datos personales por particulares y entidades financieras en México

Para identificar propiamente quienes son los particulares y en qué se diferencian de las entidades financieras, se debe comprender quienes realizan el tratamiento de datos personales de los usuarios. Si bien ambos realizan tratamiento de datos personales, en México se diferencia claramente los particulares de las entidades financieras por las formas en cómo se ha ido adecuando la ley en nuestro país. Por supuesto que se corre un gran riesgo cuando no se protege debidamente los datos biométricos ya sea por uno o por otro, pero en México la distinción entre particulares, entidades financieras y sujetos obligados es claramente delimitado con sus leyes específicas.

1.3.5.2 El caso de la excepción de las Entidades Financieras de los sujetos regulados de la Ley Federal del Protección de Datos Personales en Posesión de Particulares

Resulta interesante el atender el caso de las Entidades Financieras, tal como las Sociedades de Información Crediticia y las Entidades de Tecnología Financiera, en relación con los particulares. El punto es que tanto a las Entidades Financieras como a los particulares, les son aplicables leyes distintas, tanto del derecho financiero por un lado, como derechos particulares por otro, y por lo tanto, se complica identificar frente a qué autoridad se debería acudir en caso de un mal tratamiento de datos personales, comprendiendo que el Órgano Constitucional Garante de la protección de datos es el INAI, pero que como se verá a continuación, dentro del ecosistema

financiero, existe una serie de autoridades que intervienen y que no son precisamente especialistas en datos personales, y por lo tanto, pudiera comprometerse el respeto al derecho de privacidad de los titulares.

Primeramente se debe mencionar el caso de los particulares para diferenciarlos de una entidad financiera. Los particulares, de acuerdo a la LFPDPPP en su artículo 2° son todas aquellas personas físicas o morales de carácter privado que con fines de lucro, lleven a cabo el tratamiento de datos personales. La ley aplicable a los particulares cuando realizan tratamiento de datos lo es la LFPDPPP publicada en el año 2010, mientras que la autoridad encargada de garantizar el derecho de protección de datos personales para la resolución de solicitudes vía recurso de revisión es el INAI quien recibe, atiende y da trámite a las inconformidades de los titulares de datos personales ante el tratamiento de los responsables del uso de los datos. Una instancia superior, lo es a través del juicio de nulidad, que de acuerdo al artículo 56° de la LFPDPPP establece que será a través del Tribunal Federal de Justicia Administrativa, quien es el encargado de regular las funciones administrativas de las autoridades responsables de vigilar el cumplimiento de las leyes por el INAI en este rubro. Posteriormente, es posible acudir a la protección constitucional del juicio Amparo en caso de transgresión a los derechos humanos como lo es la privacidad y protección de datos personales. De acuerdo a José Soto Galindo, en su nota de “el Economista” menciona que es de suma importancia “el adecuar la regulación a la jurisprudencia de la Segunda Sala de la Suprema Corte que determinó que contra las resoluciones del INAI en materia de protección de datos lo conducente es el juicio de amparo y no el juicio de nulidad”[35]

Por otro lado, para comprender lo que son las entidades financieras, tendremos que remitirnos a la *Ley de Instituciones de Crédito*, donde se describe en el artículo 1° que son todas aquellas que ofrecen el servicio de banca y crédito. Esta ley regula la organización y funcionamiento de dichas instituciones, así como las actividades y operaciones que las mismas podrán realizar en su sano y equilibrado desarrollo, así como garantizar la protección de los intereses del público de acuerdo a los términos del Sistema Bancario Mexicano. El servicio de banca y crédito sólo podrá prestarse por instituciones de crédito, las cuales son: Instituciones de banca múltiple, y las

[35] José Soto Galindo “protección de datos personales” *https://www.eleconomista.com.mx/opinion/Proteccion-de-datos-personales-20220102-0004.html*

Instituciones de banca de desarrollo. Estas entidades financieras se encuentran bajo la supervisión de diversas autoridades, tal como el Banco de México, la Comisión Nacional Bancaria y de Valores, la Secretaría de Hacienda, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros y la Procuraduría Federal del Consumidor, así como de institutos como la Institución Mexicana para la Competitividad, o el comité donde participa la sociedad civil a través de distintas asociaciones. Siendo el caso de tratamiento de datos personales, específicamente los datos biométricos, estos se dan mayormente en la celebración de contratos para apertura de cuentas bancarias nivel 4, así como para créditos al consumo y comerciales, particularmente de manera remota; es por ello que el marco regulatorio de las entidades financieras, robustece los requisitos de carácter biométrico al observar en el procedimiento que se sigue para la verificación de identidad y la captura de documentos de identificación, incluyendo los provenientes de registros de autoridades mexicanas. Lo interesante en esta cuestión, es que si bien existen diversas resoluciones como la resolución que modifica las disposiciones de carácter general aplicables a las instituciones de crédito[36] donde establece los lineamientos en torno a los datos biométricos, en caso de un mal tratamiento, estas entidades financieras no están supeditadas a la autoridad del INAI, sino al CNBV, cuestión que complicaría de alguna forma el ejercicio de los tan renombrados derechos ARCO que garantizan la autodeterminación informativa.

Con respecto a las entidades financieras se debe considerar que el manejo de datos que realizan, desde un enfoque legalista de acuerdo a las leyes aplicables en este rubro, no es el mismo que llevan a cabo los particulares en general, debido a que si bien no es posible compartir a terceros la información personal relativa a los clientes, la *Ley de Instituciones de Crédito* tampoco prevé el corregir o eliminar cierta información, siendo un ejemplo claro las relaciones patrimoniales de cada cliente; y a pesar que la Ley en comento establece la cláusula relativa a la protección de datos en todos los contratos que celebre el titular de los datos biométricos con los Bancos y las Instituciones Financieras, están obligadas a informar a los titulares de las cuentas y titulares de sus datos personales proporcionados, de los cambios y el tratamiento que se les esté dando a dichos datos personales. Es por ello que resulta

[36] Diario Oficial de la Federación RESOLUCIÓN que modifica las Disposiciones de carácter general aplicables a las instituciones de crédito. *https://www.dof.gob.mx/nota_detalle.php?codigo=5602349&fecha=12/10/2020*

de suma importancia que los titulares identifiquen cuáles datos personales y/o biométricos están otorgando, y en su caso, puedan ejercer sus derechos ARCO ante las instituciones de protección pertinentes, ya que independientemente del sujeto que maneje los datos, sea persona física, jurídica o una entidad financiera, los datos personales contienen una relación de todo lo que refiere el patrimonio de los clientes o usuarios como personas físicas, como titulares, los cuales son reconocidos por igual en la Constitución Mexicana y la LFPDPPP como tales, y que es donde precisamente se podría ajustar en los contratos con las entidades financieras, que se supeditarán ante la jurisdicción del INAI.

Las Instituciones Financieras están obligadas a informar a los titulares sobre el manejo de sus datos personales proporcionados de acuerdo a las leyes mexicanas y por lo tanto deberían supeditarse a las autoridades de transparencia y protección de datos establecidas para ello, tal como cualquier particular. Las entidades financieras no deberían permanecer ajenas a la regulación en materia de datos personales ni a la autoridad del INAI. Lo idóneo es que todo el sector financiero quede regulado desde la legislación de datos personales y sujetos a la autoridad del INAI, en materia de datos, sin que haya ni regulación ni autoridades paralelas, como la CNBV interviniendo o pronunciándose sobre temas de datos personales.

Por otro lado, también existen las Sociedades de Información Crediticia, que están reguladas por la *Ley para Regular las Sociedades de Información Crediticia* y demás disposiciones aplicables, principalmente del sector financiero. Los burós de crédito, como es conocido comúnmente, realizan un tratamiento amplio de datos personales, existiendo la posibilidad de que se vulnere el derecho a la autodeterminación informativa. Las Autoridades Financieras que participan en el ecosistema de las Instituciones de Tecnología Financiera, donde se exenta al INAI como autoridad de datos personales, recaen en:

- Banco de México
- Comisión Nacional Bancaria y de Valores (CNBV).
- Comisión Nacional de Seguros y Fianzas (CNSF).
- Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR).
- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF).

- Secretaria de Hacienda y Crédito Público (SHCP).

Es importante mencionar que también existe la *Ley para Regular las Instituciones de Tecnología Financiera,* donde se incluye la regulación de las *FINTECH,* entendidas como "industria naciente en la que las empresas usan la tecnología para brindar servicios financieros de manera eficiente, ágil, cómoda y confiable. La palabra se forma a partir de la contracción de los términos *finance* y *technology* en inglés."[37] Este tipo de instituciones de tecnología financiera ofrecen diversos tipos de servicios financieros, operando dentro de diversos mercados. Algunas empresas ofrecen sus servicios directamente a los usuarios del sistema financiero y otras diseñan soluciones para otras empresas. Cabe resaltar que las Instituciones de Tecnología Financieras, a decir del libro del INAI denominado *"Recomendaciones para el tratamiento de datos personales y cumplir con el deber de seguridad para Instituciones de Tecnología Financieras"*[38], con la entrada en vigor de la normativa para regular las Instituciones de Tecnología Financiera, las Instituciones de Financiamiento Colectivo (IFC) y de Fondos de Pago Electrónico (IFPE) son reconocidas como personas físicas o morales de carácter privado, y por lo tanto, se convierten en sujetos obligados a cumplir con la normativa en protección de datos personales conforme a lo que se establece en la *LFPDPPP* así como su Reglamento. Lo que significa que las personas físicas o morales privadas, que traten datos personales en las actividades de estas Instituciones de Tecnología financiera se ven obligadas a cumplir una serie de obligaciones establecidas en la ley en comento, con objeto de garantizar a los titulares el derecho a la protección de su información personal, siendo el INAI la autoridad regente de velar por el respeto de estos derechos. Cuestión curiosa que mientras otras entidades financieras no están supeditadas al órgano constitucional garante, las *fintech* si lo están, quedando pendiente que poco a poco las mismas entidades financieras se subordinen al INAI por ser el órgano facultado para la protección de datos personales.

---

[37] FINANZAS + TECNOLOGÍA = FINTECH. Las empresas FinTech ofrecen diversos tipos de servicios financieros y operan dentro de mercados variados. Algunas prestan sus servicios directamente a los usuarios del sistema financiero y otras diseñan soluciones para otras empresas. *¿Qué es FINTECH? https://www.fintechmexico.org/qu-es-fintech*

[38] Recomendaciones para el tratamiento de datos personales y cumplir con el deber de seguridad para instituciones de tecnología financiera (ITF), INAI, febrero 2021, p. 14 *https://home.inai.org.mx/wp-content/uploads/TratamientoDP_FINTECH.pdf*

Es notable señalar la forma en cómo se regulan las relaciones de los sujetos económicos y el avance de las nuevas tecnologías, debido a que la inercia misma de ambas, no sólo parece avanzar estrepitosamente en una simbiosis entre la economía de datos y las nuevas tecnologías, sino que ya está dentro de ellas o *siempre* ha estado dentro de ellas, un área donde se mezclan intereses diversos y hay que estar muy atentos a su progreso, anteponiendo siempre el derecho a la privacidad y protección de datos personales.

1.3.5.3 La Comisión Nacional Bancaria y de Valores (CNBV) y la modificación a la Circular Única de Bancos (CUB) en cuanto al fomento, implementación y regulación del uso de datos biométricos para instituciones financieras

También es cierto, que aunque las entidades financieras no están supeditadas a la ley de protección de datos en posesión de particulares y por lo tanto a la autoridad del INAI, no hagan nada por proteger los datos de sus clientes. Al contrario, existe mucha disposición de hacerlo proactivamente. En agosto de 2017, la CNBV publicó una serie de cambios a la Circular Única de Bancos, teniendo como objetivo el combatir el robo de identidad dentro del sector bancario. Estos aspectos incorporaron y regularon el uso de datos biométricos (siendo la huella dactilar la que principalmente se reconozca) para la autenticación de los usuarios de la banca. Se implementó estas cuestiones debido a la necesidad de fortalecer los procedimientos y mecanismos que las instituciones de crédito utilizan para identificar a los usuarios que contratan algún tipo de servicio o producto, para así prevenir y detectar fraudes como la suplantación de identidad. Es importante mencionar que las instituciones financieras pueden integrar una base de datos biométricos de sus clientes, apoyándose en un inicio de la verificación en línea que pueden hacer con el INE, para corroborar principalmente la huella digital del usuario en algunos procesos específicos. Posteriormente los bancos pueden disponer de esa base de datos para autenticar a sus clientes al realizar operaciones y contrataciones. Cabe mencionar que aunque no se reconocen el tratamiento de datos personales, si se identifican como datos transaccionales, pero se diferencian por cuestiones legalistas.

Los aspectos de mercado surgidos del uso de tecnologías biométricas por parte de actores privados o particulares requieren un estudio especializado; empero, cabe puntualizar que, tal como lo menciona Marianne Díaz, no es posible realizar una separación precisa entre los tratamientos privados y públicos de los datos

biométricos, ya que la implementación de estas tecnologías pasa a través de procesos de contratación con actores privados, quienes mantienen intereses y motivaciones meramente económicas. Y más aún, al hablar de las entidades financieras privadas, es más difícil que cuenten con intereses sociales, que como ya se vio, incluso la propia ley mexicana en esta materia financiera, funciona y trabaja bajo esquemas especializados, quedando exenta de su inclusión de tratamiento de datos personales como aquellos regulados en la LFPDPPP, permitiendo así que dichas instituciones financieras mantengan sus propios esquemas y protocolos de manejo de datos biométricos.

1.4 Referencias en la legislación Europea Vigente y España

Se decidió basar la comparación jurídica entre el viejo continente, España y México debido a que como es bien sabido, Europa y España son referentes obligados en materia de regulación de datos personales, aspecto que en México, a pesar de tener más de una década de regularlos frente a particulares, no se ha definido, especificado ni mucho menos regulado el tratamiento de datos biométricos, por lo que con fundamento en el método de estudio del derecho comparado, es que se procederá a realizar dicho análisis, para obtener resultados que seguramente serán de gran beneficio para nuestro país debido al desarrollo imparable de la época digital que avanza en el mundo.

1.4.1 Antecedentes de la Legislación Europea

En relación con la Unión Europea es preciso mencionar como antecedente que Alemania y Suecia tiene el reconocimiento de ser los pioneros de la era de las leyes sobre protección de datos. Estas leyes generalmente son mencionadas como la primera generación de leyes sobre protección de datos. La Ley de Suecia de 1973 reflejaba la preocupación de la época sobre el uso de sistemas de información. Posteriormente entre los años 1980 y 1990 se da el mayor avance en esta materia. La base del trabajo desarrollado durante tal período encuentra su cumbre en el Convenio sobre Datos Personales del Consejo de Europa de 1980[39] un Convenio que buscaba generar una legislación relativamente uniforme en toda Europa. Aunque en

[39] Convenio de 28 de enero de 1981, del Consejo de Europa para la protección de las personas en lo referente al tratamiento automatizado de los datos personales. *https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales*

retrospectiva el Convenio del Consejo de Europa suministró una sólida fundamentación para la protección de los datos en Europa, no tuvo el éxito esperado, debido a que no todos los miembros del Consejo de Europa consideraron que el Convenio les obligaba a cumplir con una ley interna. El 28 de enero de 1981 fue establecido el Convenio del Consejo de Europa en Estrasburgo para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, que posteriormente sería conocido como el Convenio 108. Este Convenio trata de conciliar la libre circulación de la información con el respeto de la vida privada, estableciéndose una perspectiva innovadora y contemporánea de protección de los derechos humanos y de las libertades fundamentales. No fue sino hasta 1995 que la Directiva sobre tratamiento de datos personales fue adoptada en Octubre de ese año. El objeto y fin del Convenio se reconoce en su artículo 1º el cual es: "el garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos)"

La Unión Europea se convirtió en el impulsor de la protección de datos, obligando a sus Estados miembros a implementar la Directiva y conduciendo a terceros países a adoptar los mismos principios, principalmente con el fin de promover el comercio electrónico. El positivo impacto de la Directiva Europea de Datos Personales se manifestó. La protección de datos personales mediante la legislación se ha transformado en una institución legal permanente en cada país. La relación del individuo con la sociedad y otras organizaciones se enmarca en un ambiente de operaciones que incluye el derecho a la protección de los datos. Y este derecho finalmente es reconocido como un derecho fundamental.

Es por ello que en materia de protección de datos, Europa es el pionero en establecer los lineamientos legales en datos personales, desde la *"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"* que fue aprobada en 1995, la cual se fue actualizando en la forma de convenios, directivas o decisiones para adaptarse

a los avances de la tecnología, hasta el 2016 que tras un largo periodo legislativo se derogó la legislación previa, la Directiva 95/46/CE, para aprobar un nuevo *Reglamento General de Protección de Datos* 2016/679 o RGPD, 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, siendo de aplicación obligatoria para cada empresa y administraciones públicas de cada estado de la Unión Europea en el segundo trimestre del año 2018. Se compone de 11 capítulos, 99 artículos y 173 considerandos.

Como se va a estudiar el más reciente RGPD de la Unión Europea, es necesario ahondar en las novedades que se han incluido con respecto a la anterior directiva de 1995, las cuales son:

- Consentimiento y derechos de los usuarios. La legislación establece que el consentimiento debe prestarse de forma explícita mediante una acción de confirmación. De igual forma, el artículo 17 establece que los derechos se renuevan para facilitar el derecho al olvido y al de portabilidad de los datos.
- Privacidad desde el diseño y por defecto. El artículo 25 indica al responsable del tratamiento de datos, aplicar en todo el proceso del tratamiento medidas técnicas y organizativas respectivas, a fin de aplicar de garantizar la protección de datos.
- Medidas de seguridad. Aunque no se especifican niveles de seguridad, se establecen medidas en base a ciertos criterios, como son la naturaleza y alcance del tratamiento, los costes de aplicación y los riesgos.
- Evaluaciones de Impacto. Cuando se vaya a implantar un nuevo sistema tecnológico, la ley obliga al responsable del sistema a realizar una evaluación de impacto en relación con la protección de datos de carácter personal
- Ámbito de aplicación. Se prevén nuevas situaciones en las que se aplica la norma, en los casos que este reglamento sea aplicable.
- Régimen sancionador. Establece nuevas sanciones más fuertes con respecto al reglamento anterior
- Obligación de informar sobre vulneraciones de la seguridad. Se especifica la obligación por parte del responsable a informar sobre brechas de seguridad a la autoridad de control.

- Figura del delegado de protección de datos (*Data Protection Officer*). Se obliga a todos aquellos organismos o instituciones donde se lleve a cabo un tratamiento a gran escala de datos de carácter personal sensible o especiales según el art. 9 (salud, genéticos, biométricos, origen racial o étnico, opinión política, religión o creencias filosóficas, pertenencia a sindicatos, vida y orientación sexual) a crear un delegado de protección de datos.

1.4.2 Antecedentes de la legislación Española

Previo a la adaptación de la legislación interna a lo establecido por el Parlamento Europeo, la legislación española ya había desarrollado una serie de normativas en relación al tratamiento de datos de carácter personal, incluyéndose en ellos los datos biométricos. Estas normativas están basadas en la ley orgánica de protección de datos, su reglamento de desarrollo y las instrucciones y resoluciones de la Agencia Española de Protección de Datos AEPD bien conocida en aquel país.

Las leyes de protección de datos en España han evolucionado desde hace ya varios años, iniciando con la Ley Orgánica De Regulación Del Tratamiento Automatizado De Los Datos De Carácter Personal de 1992 (LORTAD), luego se dio la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal de 1999 (LOPD) y posteriormente la ley actual Ley Orgánica de Protección de Datos y de Garantía de Derechos Digitales de 2018 (LOPDGDD) en la que se basa el estudio comparativo de esta investigación.

En primera instancia, la LORTAD se reconoció como *Ley Orgánica 15/1999*, de 13 de diciembre del año en cita. Se trata de las normativas iniciales y esenciales en cuanto a la protección de datos personales en España. Para su protección se estableció una serie de principios de obligado cumplimiento para todas aquellas entidades estatales u organizaciones particulares, que traten datos de carácter personal para el desarrollo de su actividad.

Posteriormente, se dio la segunda legislación conocida como LOPD. Esta ley obligó a todas las empresas, personas y organismos tanto privados como públicos, que dispongan de datos de carácter personal a cumplir una serie de requisitos y aplicar determinadas medidas de seguridad en función del tipo de datos que posean. A grandes rasgos, las obligaciones legales fundamentales fueron dar de alta los

ficheros en la AEPD, elaborar y mantener actualizado el Documento de Seguridad y obtener la legitimidad de los afectados.

Luego, a unos meses de haberse aprobado el último reglamento de la Unión Europea, el RGPD, el Congreso español decidió aprobar una nueva ley que adapte el ordenamiento español a dicho reglamento. Es entonces cuando se dio la LOPDGDD, normativa que incluye algunas novedades en cuanto a los principios de la protección de datos, el tratamiento de los mismos, entre otros. Dentro de los 97 artículos dispuestos en esta Ley Orgánica, se pueden encontrar algunos puntos relevantes como los derechos digitales, tal como el derecho al olvido, el acceso digital a los menores edad, derechos a la neutralidad de la ley o el derecho al testamento digital, entre otros.

1.5 Conclusiones preliminares del capítulo I

La historia, la doctrina, la investigación y los avances científicos y tecnológicos reconocen e identifican muy bien lo que es la biometría y los datos biométricos, ya que desde hace mucho tiempo se han utilizado como un medio para autenticar o verificar la identidad de una persona a través de su fisionomía o de sus rasgos de comportamiento.

Las referencias de las conceptualizaciones de privacidad, intimidad, datos personales y datos sensibles permiten comprender que todas éstas se encuentran implícitas en los datos biométricos que son tratados como motivo de identificación o autenticación, y por lo tanto estarían comprometidas al momento en que se les brinde algún tratamiento, lo que sería prudente el reconocerse y especificarse en toda ley.

El haber hecho un repaso por las generalidades del funcionamiento de los sistemas biométricos permite comprender de forma mucho más integral los puntos clave dentro del procesamiento de información biométrica, sobre todo al momento de reconocer los estándares de calidad y de ciberseguridad por los que cualquier empresa u organización debe considerar, ya que si se cumplen debidamente, en conjunto con buenas prácticas como la privacidad por diseño y por defecto, se evitarían brechas de seguridad de los datos, y por lo tanto se evitarían las responsabilidades legales que cada país establece en su legislación.

Por otro lado, tanto el sistema jurídico anglosajón como en el sistema romano-germánico, son buena referencia previo al estudio a fondo de la comparativa entre Europa, España y México, ya que permite identificar los puntos en común en torno a dichos conceptos, las autoridades involucradas, los sistemas de identificación o bases de datos, así como los mecanismos legales para exigir el respeto al derecho de privacidad. En el caso anglosajón, sobresale la tan vasta doctrina que establece el derecho a estar solo o *privacy*, en donde realizan un estudio pormenorizado entre vida privada, intimidad e intimidad exclusiva, y que puede tomarse como referencia al momento de enriquecer el concepto de datos personales sensibles. A pesar que en países como en Estados Unidos no cuenten con leyes específicas de protección de datos, eso no exime que tengan lineamientos para garantizar el derecho a la privacidad, y mucho menos que no puedan ser tomadas como referencia para hacer valer el derecho humano a la privacidad en nuestro país, ya que al momento de estudiar las políticas de privacidad que cada organización o empresa tiene, o las propias instituciones gubernamentales de registro y seguridad que así se vean involucradas, ofrece muchas luces sobre cómo garantizar la privacidad de las personas. Por otro lado, los países latinoamericanos consultados dan ejemplo sobre cómo es posible designar autoridades especializadas en la materia, así como implementar sus propios sistemas de identificación y registro de datos biométricos con fines de seguridad, que se encuentren a la altura de las necesidades actuales.

El caso de las Entidades Financieras y los particulares es de suma importancia, ya que finalmente, ambos dan tratamiento y sacan provecho de los datos personales de los usuarios, y éstos siempre tienen el mismo carácter: siempre son datos personales, siempre pertenecen a los derechos humanos debido a que giran en torno a los derechos de la personalidad tan importantes como lo es la privacidad y la intimidad, y por lo tanto debería homogeneizarse la jurisdicción de la autoridad designada constitucionalmente para ello, tal como el INAI.

Finalmente, las referencias obligadas de Europa y de España en materia de protección de datos, son necesarias para comprender su bien jurídico tutelado, como lo es la privacidad y los datos personales, y que de alguna forma han alcanzado una madurez a través del RGPD.

CAPÍTULO II. ESTUDIO DE LOS REGLAMENTOS Y LEYES DE PROTECCIÓN DE DATOS PERSONALES DE EUROPA, ESPAÑA Y MÉXICO EN RELACIÓN A LA PROTECCIÓN DE DATOS BIOMÉTRICOS

Sumario: 2.1. Generalidades de los Sistemas Jurídicos referidos 2.2. Sujeto materia de comparación: los datos biométricos y su relación con los datos personales y las categorías especiales de protección de datos en las legislaciones de la Unión Europea y España 2.3. La macrocomparación como nivel de comparación de los datos sensibles en las legislaciones de Europa, España y México 2.4. Resultados del contraste de las leyes de Europa, España y México

En el presente capítulo, se procederá a realizar el estudio de derecho comparado con base en la metodología comparatista conocida como macrocomparación[40]. Se abordará el estudio de la comparación de derechos, entre la legislación Europea y Española en materia de protección de datos personales, específicamente en los datos biométricos, para compararlo y contrastarlo con la legislación Mexicana de Protección de Datos en Posesión de Particulares. Lo anterior para identificar los supuestos que la legislación mexicana pudiera incluir en materia de datos biométricos.

2.1 Generalidades de los sistemas jurídicos referidos

Se ha seleccionado a la Unión Europea y España como punto de comparación y referencia, dado que son quienes cuentan no solamente con leyes y reglamentos vigentes en esta materia, sino porque cuentan con mecanismos jurídicos de protección de datos, incluyendo los denominados datos biométricos. Para definir el otro extremo comparado, es que se recurre a México, donde se estudiará la concepción que se tiene con respecto a los datos personales, sus distintas categorías como datos sensibles, y si es que incluye o no textualmente hablando, el concepto de

[40] "La macrocomparación es la comparación entre dos o más sistemas jurídicos. Este tipo de comparación no sólo consiste en comparar dos o más sistemas jurídicos, sino que comprende los métodos y procedimientos que conforman un sistema legal. Las diferentes técnicas legislativas, medios de interpretación, decisiones judiciales, estilos de codificación, procedimientos judiciales u organización judicial son elementos que integran un sistema. Al realizar una comparación en gran escala se debe tomar en cuenta todos los factores que integran un sistema jurídico." Adrián Mancera Cota, *Boletín Mexicano de Derecho Comparado. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332008000100007*

datos biométricos dentro de su regulación, al igual que entablar mecanismos jurídicos para su de protección.

Se perdería objetividad si se estudiase directamente las leyes de protección de datos de los países aludidos si no se acude a la metodología que el derecho comparado sostiene, lo cual es identificar las características de los sistemas jurídicos a comparar, por lo que en primer punto, se identificará el sistema jurídico al cual pertenecen la Unión Europea y los Estados aludidos, en segundo lugar se ubicará el sujeto materia de comparación, siendo por supuesto la especificidad de los datos biométricos; en tercer lugar, a través de la macrocomparación, se identificará la delimitación del nivel de comparación; y en cuarto lugar se obtendrá la delimitación de nivel de comparación de los datos biométricos en las legislaciones de la Unión Europea, España y México. Por supuesto haría falta una quinta parte, una prueba de funcionalidad en la que, tal como lo menciona Adrián Mancera Cota, autor en quien se basa la presente metodología comparatista, sería el momento en que debería responderse si sería posible determinar la factibilidad de adoptar una solución extranjera por medio de dos preguntas: "primera, si ha resultado satisfactoria en su país de origen y, segunda, si funcionará en el país donde se propone su implantación"[41] cuestión que se abordará llanamente en el Capítulo III de esta investigación.

A continuación se procederá con las cuatro etapas del sistema comparativo antes mencionado para determinar la factibilidad de adoptar la solución extranjera de datos biométricos en nuestro país.

2.1.1 Sistema Jurídico de la Unión Europea

Por un lado, tenemos a la Unión Europea, una organización de naciones compleja de definir, pero acudiendo a especialistas como Nuria González se menciona que “la Unión Europea no es un Estado, ni una federación de Estados y tampoco es una organización internacional. Hay un sector doctrinal que la conceptualiza como un sistema de soberanías compartidas, un poder civil basado en la interdependencia que dispone de poderes normativos”[42] También se ha referido a

[41] Adrián Mancera Cota “Consideraciones durante el proceso comparativo” 2007 *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332008000100007*

[42] González Nuria Martín “Sistemas jurídicos contemporáneos” *Nostras Ediciones,* México p. 170 *https://bibliotecavirtualceug.files.wordpress.com/2017/06/sistemas-juridicos-nuria-gonzalez.pdf*

la integración europea como Europa comunitaria, debido a que cuenta con elementos democráticos (Parlamento) y elementos tecnocráticos (Comisión Europea). Es por ello que si la Unión Europea podría situarse en algún sistema jurídico, definitivamente encuadra con el Derecho comunitario, ya que se impone a los Estados miembros[43]. Al ser un derecho comunitario que cuenta con los atributos de codificar la ley en cuerpos legislativos, donde la aplicación de la misma se emplea el precepto que mejor se adapte al caso y en la interpretación se explican disposiciones normativas, se reconoce por lo tanto como un derecho romano-germánico.

En relación con los mecanismos jurídicos de la Unión Europea para garantizar la protección de datos personales, como ya se ha mencionado, el actual RGPD de Europa vino a sustituir la antigua reglamentación de 1995 conocida como *"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"* la cual no contenía referencia alguna a los datos biométricos. Hacía mención en su artículo 2 en cuanto a los datos personales[44] que en su forma más extensiva consideraba como dato personal la identidad física, fisiológica, psíquica, cultural y social. En ese orden de ideas, este tipo de identificación a través del cuerpo se puede relacionar con el concepto de datos biométricos, pero sin duda existía una laguna de ley en cuanto a especificar el dato biométrico del titular, reconocido en esta ley como el interesado.

Posteriormente, una vez que entró en vigor el RGPD, se abordaron temas actualizados que sustituyeron la reglamentación anterior. El reglamento en comento tiene como objetivo principal el proteger los derechos y las libertades de las personas físicas en relación con el procesamiento de sus datos personales, y al ser un reglamento de aplicación general en Europa, el cual es aplicable a los 27 países integrantes del mismo, buscando reforzar y garantizar el mismo nivel de protección de datos personales en los territorios de los Estados miembros.

---

[43] *Idem*

[44] Artículo 2. Definiciones: A efectos de la presente Directiva, se entenderá por: a) «Datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o vario elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social; (…) *https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/18.pdf*

Dado que el objetivo del reglamento es dar a los residentes de la Unión Europea el control de sus propios datos, este reglamento regula la forma en que las personas y empresas recopilan, procesan, almacenan y eliminan datos personales de los residentes en cualquier Estado de la Unión Europea. Por lo tanto su aplicación no solo tiene implicaciones para las empresas dentro de Europa, sino que también para cualquier persona o empresa extranjera que procese o almacene datos de los residentes de la Unión Europea. Se toma como referencia esta reglamentación en materia de datos biométricos con el objetivo de extraer sus avances y compararlos con la legislación mexicana, siendo precisamente el artículo 4, apartado 14 del reglamento en comento, en donde se defina claramente la conceptualización de datos biométricos: "«datos biométricos»: 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 confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;" Dentro del referido reglamento, se hace alusión a los datos biométricos sobre algunas especificaciones de su tratamiento, cuestión que se abordará posteriormente.

2.1.2 Sistema Jurídico de España

El sistema jurídico Español encuadra en lo que se conoce como sistema continental de Derecho en clara referencia europea. También es conocido este derecho continental como *civil law* y tiene su origen en el derecho romano, germano y canónico. Su principal característica es la esencialidad de un código de leyes escrito, es decir, que el sistema normativo esté codificado y este sea su principal fuente de derecho. Oficialmente conocido como Reino de España, es un país soberano constituido en un Estado social y democrático, teniendo su forma de gobierno como monarquía parlamentaria, y que aunque es un país unitario, funciona como una federación descentralizada de comunidades autónomas, cada una de ellas con diferentes niveles de autogobierno. Es un Estado de Autonomías, y cuenta con un parlamento bicameral conocidas como Cortes Generales. Trazan la separación del sector público y privado del ordenamiento jurídico. Al Reino de España ser parte de uno de los 27 países miembros de la Unión Europea, se encuentra vinculado al cumplimiento de los lineamientos europeos, y por lo tanto al RGPD y al Comité Europeo de Protección de Datos creado al margen de esta ley.

Se decidió estudiar el Reino Español por los avances que dicho Estado ha realizado en materia de protección de datos personales. Cabe mencionar que dicho país ha sido el primer Estado Miembro de la Unión Europea en adecuar su legislación en materia de protección de datos al reglamento comunitario. En España, tal como se comentó previamente, existió una importante evolución reglamentaria en esta materia, siendo la LOPDGDD de 2018 la que actualmente sea aplicable y vigente en aquel país. Cabe mencionar que esta ley, si bien es cierto perfecciona los modelos identificables de tratamientos de datos personales y de entro de ellos identifica como categoría especial a los datos biométricos ya mencionados de forma general en el RGPD, no hace alusión directa a los datos biométricos como lo fue en la LOPD del 2007. Esto por supuesto no significa que quedan exentos de su aplicabilidad cuando se realice algún tratamiento de los datos biométricos. Lo que pasa es que habrá que determinar la técnica aplicada para dicho procesamiento, ya sea por el método de identificación biométrica (uno-varios) o autenticación biométrica (uno a uno)[45] siendo objeto de análisis de la misma Agencia Española de Protección de Datos a través del grupo de trabajo del artículo 29, donde analizan las funciones del delegado de protección de datos.

Se toma como referencia esta ley para estudiar su contenido en torno a la protección de datos biométricos.

2.1.3 Sistema Jurídico de México

México, cuyo nombre oficial es los Estados Unidos Mexicanos, es una República Federal integrada por 32 estados independientes. Se sabe que su sistema jurídico pertenece a la tradición romano-germánico, debido a la codificación de normas jurídicas y por la influencia española derivado de la conquista. Es un país soberano constituido en un Estado social y democrático, donde la forma de gobierno es una república federal presidencialista. El gobierno de México está estructurado en tres niveles, tal como el gobierno federal, el gobierno estatal y el gobierno municipal. La Unión federal también refleja la división de los tres poderes del Estado, que son el ejecutivo, el legislativo y el judicial. La rama ejecutiva del gobierno está integrada por el Presidente de México quien nombra a sus propios miembros del Gabinete, y que

[45] Gerard Arnauda Padró “Datos biométricos: ¿categoría especial de datos o no?” *PRODAT*, España *https://www.prodat.es/blog/datos-biometricos-categoria-especial-de-datos-o-no/*

no sólo es el jefe de Estado, sino también el comandante en jefe de las fuerzas armadas. Por otro lado, el Poder Legislativo está compuesto por el Senado, el Congreso de la Unión y la Cámara de Diputados. Entre las funciones del Poder Legislativo están la creación y modificación de las leyes del país y la aprobación del presupuesto nacional. El Poder Judicial del gobierno está integrado por la Suprema Corte de Justicia que a su vez está integrada por 11 jueces que ejercen las funciones de ministros de la corte, junto con un robusto sistema judicial organizado por el Consejo de la Judicatura Federal.

En relación con la protección de datos personales, se tuvo una primer referencia en el año 2007, cuando por primera vez se incorporó como derecho humano en nuestra Constitución en el artículo 6°, siendo las fracciones II y III del citado artículo donde se señaló que: “la información a que se refiere la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes”, además que: “toda persona tendrá acceso a sus datos personales o a la rectificación de éstos respectivamente”, dando como origen el primer acercamiento de éstas prerrogativas. Posteriormente mediante la reforma constitucional del año 2009 a los artículos 16 y 73, se vuelve a reconocer al derecho de protección de datos personales pero ahora a través de su procedimiento de Acceso, Rectificación, Cancelación y Oposición, al igual que facultando al Congreso para legislar en la materia. Con la reforma al artículo 16 se estableció que: “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.” Una vez identificado el derecho de protección de datos personales de las personas en la constitución mexicana, es que se codificó la LFPDPPP, siendo precisamente esta ley la que profundizara a detalle los medios de garantía de protección de datos que la constitución ya había reconocido previamente.

2.1.4 Sistemas jurídicos compatibles

Una vez identificada brevemente la naturaleza de cada uno de los sistemas jurídicos de la Unión Europea, España y México, y que posteriormente se analizará

concienzudamente con la metodología de la macrocomparación, se puede declarar que si bien es cierto la Unión Europea sería el único que pertenece a un sistema jurídico distinto como lo es el derecho comunitario, al mismo tiempo se considera mayormente de naturaleza romano-germánico debido a que cuenta con leyes codificadas que establecen principios y lineamientos a seguir por todos los integrantes de la Unión. Por lo que se concluye que es compatible y viable su comparativa con España y México debido a que éstos últimos, también cuentan con el sistema jurídico de tradición romano-germánico, y por lo tanto debido a dicha similitud, no existe limitante alguno de compararlo y contrastarlo con el sujeto materia de comparación: los datos biométricos, estudio que a continuación se procederá a analizar.

Es de suma importancia el dilucidar este tema para proponer una reforma legal a la LGPDPPP donde se incluya dentro de su articulado la especificidad de los datos biométricos, sobre todo por el gran avance, cambio y evolución tecnológica que la sociedad de la información está experimentando. Por supuesto, por interpretación sistemática, tal como lo ha hecho el INAI en sus resoluciones y declaraciones, se equiparan los datos personales sensibles con los datos biométricos, pero no deja de ser una ambigüedad que muchas otras regulaciones de datos personales de diversos países ya se ha incluido y especificado en su contenido. Siempre ha existido un conflicto entre el contenido de la ley y su aplicabilidad, no siendo la excepción dentro del tratamiento de datos, ya que siempre es necesario que se acompañe de alguna autoridad que vele por el cumplimiento de protección de datos, siendo precisamente el objetivo de esta pesquisa el realizar una investigación sistemática sobre cómo la reglamentación Europea y Española han avanzado en ello, para tomarlo como ejemplo en nuestro país y así confrontar el avance tecnológico, informático y digital que siempre lleva un paso adelante frente a la ley.

2.2 Sujeto materia de comparación: los datos biométricos y su relación con los datos personales y las categorías especiales de tratamiento de datos sensibles en las legislaciones de la Unión Europea, España y México

La selección de los países comparados responde a razones metodológicamente válidas: cuentan con el mismo sistema jurídico. De un extremo de la comparación se encuentra la Unión Europea y España, donde ambos convergen en la misma familia jurídica, el derecho comunitario es aplicable para todos los integrantes de la U.E. y las leyes del derecho interno español son acordes con los

lineamientos europeos. Su legislación en términos de datos personales es de las más avanzadas de los últimos tiempos dentro de este sistema jurídico, además de los mecanismos legales para garantizar su protección. Para definir el otro extremo de comparación que es la legislación mexicana, se decidió obedecer a un patrón neutral entre las legislaturas, como lo es el manejo y tratamiento de los datos personales, así como su acepción como datos personales sensibles. Al ser México el país objeto de comparación con Europa y España, es que se procede a delimitar la comparación del patrón neutral con el de datos biométricos, y obtener resultados de dicha colisión de reglamentos y leyes pertinentes.

2.2.1 Patrón neutral y datos biométricos

El patrón neutral, identificado como datos personales entre la Unión Europea, España y México es prácticamente el mismo, debido a que el legislador mexicano tomó de la legislación española los principios generales de la protección de datos personales para incluirlos en las leyes mexicanas, incluso la adecuó y le cambió algunos aspectos que quedan aún más claros (como definir al propietario de datos personales como «titular» y no como «interesado», como se menciona en las leyes europeas y que ha sido objeto de diversas críticas por la academia española) entre otras variaciones. Lo que no se incluyó en la LFPDPPP fueron reformas posteriores hechas en Europa y España en sus leyes de protección de datos, donde precisamente se reguló el tratamiento de datos biométricos y se incluyeron los derechos digitales, ni mucho menos se incluyó la categorización del tratamiento de datos personales que contiene el artículo 9 del RGPD que responde a la pregunta sobre cómo deben ser tratados los datos considerados especiales, siendo precisamente los datos biométricos como tales.

En el artículo 4° del RGPD se distinguen cuatro tipos de datos: datos personales, datos genéticos, datos biométricos y datos relativos a la salud. Si bien no define lo que son datos sensibles como lo hace la LFPDPPP, se distinguen posteriormente como categorías especiales de datos personales y categorías especiales de tratamiento, tal como lo menciona el artículo 9 del Reglamento, que es mucho más amplio que en un concepto de datos sensibles, y que a la par dice: “Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación

sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física" mencionando los supuestos en los cuales no será de aplicación cuando se den las circunstancias descritas posteriormente, como lo es el consentimiento explícito o por protección de intereses vitales del interesado, entre otros. Esta especificación como categorías especiales de datos personales del RGPD puede servir como fundamento para expandir lo definido como datos sensibles de la LFPDPPP.

Por lo tanto, aunque los datos biométricos son el punto de estudio y análisis, a falta de su mención en la ley mexicana, se debe recurrir del patrón neutral que comparten las leyes estudiadas como son los datos personales, y estudiar sus distinción y categorización de datos especialmente sensibles, con el fin de tomar el resultado de la colisión de leyes, tomando la macrocomparación como la metodología a seguir en el siguiente tema, sin perder de vista que el tópico principal son los datos biométricos regulados en las leyes de la Unión Europea y España.

2.3 La macrocomparación como nivel de comparación de los datos biométricos en las legislaciones de la Unión Europea, España y México

Aunque se considera que los sistemas jurídicos de la Unión Europea, España y México son similares al pertenecer a la tradición romano-germánica tal como se analizó previamente, es necesario remitirse a la metodología de la macrocomparación debido a que cada reglamentación respectiva cuenta con sus propios órganos legislativos, así como sus propios métodos y procedimientos que conforma el sistema legal. Que decir en cuanto al procedimiento legal de las Autoridades de control de protección de datos, las decisiones de cada una de éstas, y sus diversos medios de interpretación. Es por ello que bajo estas dos fases de la macrocomparación, en su sentido de órganos legislativos y Autoridades de control de protección de datos, es que se procederá con la tercera de las cuatro etapas del sistema comparativo utilizado en este estudio, identificando las características primeramente entre la Unión Europea y España, y luego compararlas con las particularidades de México.

2.3.1 Los órganos legislativos y las Autoridades de control de la Unión Europea y España, en materia de protección de datos.

Es necesario identificar de qué forma han sido creadas las leyes que son vigentes en la materia de protección de datos en los países a estudiar, ya que de esa forma será posible comprender más ampliamente sobre cómo están siendo aplicados los lineamientos de las mismas de forma realista. Para proceder con el análisis de los órganos legislativos que conforman el sistema legal tanto de Europa como de España, habrá que identificar primeramente cuales son los organismos de cada uno de estos, así como mencionar brevemente sus funciones.

Por lo que respecta a Europa, existe el Parlamento Europeo como representante del pueblo, y el Consejo de la Unión Europea como representante de los Estados Miembros, que entre ambos, son los que aprueban la legislación, así como presupuestos de forma conjunta, siendo la Comisión Europea la que representa los intereses y a la vez propone y ejecuta la legislación[46]

2.3.2 Autoridades de control en Europa y España

Ya en materia más específica de protección de datos, derivado del RGPD del 2016 se creó El Comité Europeo de Protección de Datos (CEPD) como un organismo independiente que garantiza la aplicación de las normas de protección de datos en toda la Unión Europea. El CEPD está compuesto por representantes de las autoridades nacionales de protección de datos de los países de la Unión Europea y del Supervisor Europeo de Protección de Datos (SEPD)[47]. La Comisión Europea también nombra un delegado de protección de datos responsable de supervisar la aplicación de las normas sobre protección de datos en la propia Comisión Europea. El Delegado de protección de datos es quien garantiza de manera independiente la aplicación interna de las normas, en cooperación con el SEPD. Cabe mencionar que el RGPD también apertura la posibilidad de que existan una o varias autoridades públicas independientes por parte de los Estados miembros, para la supervisión y la aplicación del mismo RGPD, con el fin de proteger los derechos y las libertades

[46] Comisión Europea. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es
[47] El SEPD es un organismo de la UE que se encarga de supervisar la aplicación de las normas sobre protección de datos en las instituciones europeas y de investigar las denuncias. *https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es*

fundamentales de las personas físicas, dando cabida precisamente a la Agencia Española de Protección de Datos.

Por lo que incumbe a España, su poder legislativo está a cargo de las Cortes Generales, que a su vez se subdividen en un congreso y un senado, siendo estos organismos los que dan forma a las diversas leyes en materia de protección de datos. Precisamente en este rubro es que en 1993 se creó la AEPD, fungiendo como ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones. Una vez emitido el RGPD del 2016, es que dio cabal cumplimiento al mismo fungiendo como la Autoridad de control para España, siendo precisamente ante este organismo que se lleven a cabo los procedimientos legales respectivos.

2.3.3 Los órganos legislativos y las Autoridades en materia de protección de datos de México

En relación con México, el Poder Legislativo se le ha otorgado la facultad implícita de elaborar las leyes, tal y como se expresa en la fracción XXX del artículo 73 de la Constitución, "a objeto de hacer efectivas las facultades anteriores (de las fracciones I a la XXIX) y todas las otras concedidas por esta Constitución a los Poderes de la Unión". Estas facultades referidas requieren de las facultades expresas para mantener el Estado de derecho.[48] Y precisamente lo hace a través del Congreso de la Unión, que subdividido en dos cámaras: Cámara de Diputados, y Cámara de Senadores, lleva a cabo la tarea de elaborar leyes, que a decir de Claudia Puente deberían ir conforme a una buena técnica legislativa, debido a que en México sigue siendo de poco interés el estudiar esta materia, lo cual ha traído como consecuencia un indiscriminado aumento en la producción de normas; así como la improvisación en la elaboración de documentos y la ausencia de atributos racionales de claridad, sencillez, simplicidad, generalidad y abstracción.[49]

En torno a las Autoridades en materia de protección de datos, el INAI como órgano constitucional autónomo, es el encargado del cumplimiento de dos derechos

[48] "Tales facultades le conceden el poder para abrogar, revocar y reformar las leyes del país, siempre y cuando se trate de hacer efectivas las facultades del propio Congreso conforme al artículo 73 o en otras disposiciones de la propia Constitución." Diccionario universal de términos parlamentarios http://www.diputados.gob.mx/sedia/biblio/virtual/dip/dicc_tparla/Dicc_Term_Parla.pdf p. 17

[49] Claudia Puente, *La importancia de la técnica legislativa https://forojuridico.mx/la-importancia-de-la-tecnica-legislativa/*

fundamentales: el acceso a la información pública y la protección de datos personales, disponiendo del procedimiento de protección de derechos[50] Además, en conjunto con el Sistema Nacional de Transparencia, existe la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Una vez identificadas las instituciones creadoras de normas jurídicas y las autoridades de protección de datos, se puede advertir la similitud en su funcionamiento, que tanto las Autoridades de control de la Unión Europea y España así como el Órgano Constitucional autónomo mexicano, tienen con respecto al ejercicio de sus funciones. Por lo que ahora, es pertinente proceder a la cuarta y última parte de la metodología comparativa aplicada a este tema.

2.4 Resultados del contraste de las leyes de la Unión Europea, España y México

De lo mencionado anteriormente, se advierte que tanto el poder legislativo como las autoridades de protección de datos de cada país y continente, son compatibles y viables de comparación debido a que el sistema jurídico al que pertenecen son similares, ya que promulgan leyes creadoras de instituciones y autoridades especializadas en la materia de protección de datos. En esta etapa de estudio, es el momento para identificar las similitudes y diferencias del contenido de las leyes.

En relación a los poderes legislativos de Europa, España y México, cuentan con la similitud que se basan en los principios del derecho parlamentario, debido a que están compuestos por el Parlamento Europeo, Parlamento Español y Congreso de la Unión, así como el proceso legislativo es similar. La diferencia principal radica, que mientras la Unión Europea se rige por un derecho comunitario, España y México comparten el mismo derecho civilista de tradición romano-germánica.

En torno a las autoridades de protección de datos, la similitud radica en que se cuenta con una autoridad especializada en la materia en cada sujeto internacional estudiado, lo que significa que es viable su comparativa funcional. Mientras en Europa existe el Comité Europeo de Protección de Datos (CEPD), en España se encuentra la reconocida AEPD, mientras que en México el organismo constitucional autónomo INAI. En cuanto a sus diferencias, por supuesto además de la territorialidad de

[50] Artículo 45. *Ley Federal de Protección de Datos Personales en Posesión de los Particulares http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*

aplicación de la norma, la extraterritorialidad es protegida más ampliamente en Europa y España que en México mismo. Los tres entes internacionales tienen instituciones facultadas para vigilar el manejo de datos personales y tienen de alguna forma los mismos fines a seguir. La diferencia es que la AEPD establece mayores obligaciones que la legislación le otorga para resolver las problemáticas relacionadas con la información personal, mientras que en México el problema es social y cultural, ya que muy pocos conocen las funciones del INAI y la forma en cómo ejercer sus derechos ARCO.

En relación entre España y México en cuanto a los principios que protegen los datos personales, se puede advertir que en relación a los principios que protegen a los datos de las personas, los principios son aquellos que refieren a enunciados de carácter ético cuya finalidad es mantener intacta la intimidad de los individuos al realizar un tratamiento de información. La legislación de México contempla los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. En España los principios de protección de datos personales son establecidos en la ley, así mismo sirven como una guía de carácter obligatoria para los sujetos que realizan un tratamiento de información, con el fin de no afectar a las personas en su esfera íntima. La diferencia entre ambas legislaciones en relación a los principios de protección de datos personales es que en México son establecidos en la ley, pero no son definidos, en cambio en España estos enunciados son definidos en la norma vigente para garantizar la intimidad de los individuos.

Por lo tanto, si se plantea el hecho de comparar los contenidos legales, se deberán tener en consideración 11 puntos a contrastarse, tales como:

1. Denominación de las leyes motivo de comparación
2. Objeto de la regulación: datos personales
3. Objeto específico de estudio: datos biométricos
4. Ámbitos de aplicación
5. Consentimiento
6. Aviso de privacidad y relativos en las leyes europeas
7. Principio de Confidencialidad
8. Transferencia de datos
9. Derechos de personales

10. Autoridades competentes para la protección de datos biométricos
11. Infracciones y sanciones

Como parte del estudio de cada uno de los puntos mencionados para determinar las similitudes y diferencias del contenido de las legislaciones a compararse, se tomará como patrón neutral los datos personales, donde se llega a las siguientes recapitulaciones:

2.4.1 Denominación de las leyes motivo de comparación

En la Unión Europea, como se ha venido describiendo, la ley reciente que compila los lineamientos de datos personales se denomina RGPD que fue emitido el 16 de abril del 2016, y entró en vigor hasta el año 2018 en los países miembros. Por otro lado, la última ley de España en esta materia se conoce como LOPDPGDD fue emitida el 5 de diciembre del 2018. Por lo que ve a México, su legislación vigente se le conoce como LFPDPPP promulgada el día 27 de abril del 2010. Si bien la denominación de las leyes objeto de estudio gira en torno a los datos personales, si hay consideraciones importantes al momento de contrastar su definición, ya que la ley española reconoce además los derechos digitales, cuestión que en México sigue quedando pendiente de actualización.

2.4.2 Objeto de la regulación: datos personales

El objeto de regulación de una norma jurídica es aquella cosa, situación o conducta que debe ser protegido por una ley, para cumplir ciertos fines de convivencia y relaciones sociales. Es menester aclarar que el objeto de regulación de una norma legal pretende delimitar una conducta u otorgar un mecanismo de protección específico, de ahí la importancia de señalar este criterio jurídico, el cual refiere a los datos personales, patrón neutral en la investigación por realizar la comparativa del contenido normativo de las leyes aducidas en relación con los datos biométricos.

Las tres legislaciones motivo de comparación en este análisis comparten el mismo objetivo, aunque la ley española reconoce además los derechos digitales. El contenido de los siguientes artículos es en donde se refiere al patrón neutral.

A continuación se presentan las similitudes de las leyes en torno a los datos personales, como se muestra en la tabla 2.1

Tabla 2.1

Objeto de la regulación de las leyes comparadas: datos personales y relativos

1.- OBJETO DE LA REGULACIÓN, DATOS PERSONALES		
RGPD	LOPDPGDD	LFPDPPP
Artículo 1, objeto 1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. 2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. 3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.	Artículo 1, objeto de la ley La presente ley orgánica tiene por objeto: a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones. El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.	Artículo 1.- La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Nota: Esta tabla muestra cómo el mismo objeto de las tres leyes comparadas son los datos personales, y por lo tanto son viables de compararse. *Elaboración propia*

2.4.3 Objeto específico de estudio: datos biométricos

Al ser los datos personales el patrón neutral que comparten las leyes objeto de estudio en esta investigación, es importante no perder de vista que el objeto específico de estudio son los datos biométricos. Cada ley aducida refiere a cierta categorización de los mismos de acuerdo a su concepción respectiva de cada ley, por lo cual es importante mencionar que el RGPD y la LOPDGDD comparten el mismo enfoque en relación a la categorización del tratamiento de datos personales, refiriéndolos como categorías especiales de datos personales, siendo los datos sensibles en el RGPD los siguientes: datos genéticos, datos biométricos y datos de salud, siendo el caso de la ley española el que agrega una categoría más en su

contenido, el cual es el tratamiento de datos de naturaleza penal el que se reconoce claramente en el artículo 10, que aunque se alude al mismo en la ley europea, no se clasifica como tal en su área, debido a que es la tarea de los países miembros el hecho de incluir situaciones específicas de tratamiento[51]; por otro lado, en la legislación mexicana solo se categoriza en dos ramas: datos personales y datos personales sensibles y se describen algunos de estos. A continuación se exponen los artículos que contienen las categorías especiales de datos en la tabla 2.2

Tabla 2.2

Objeto específico de estudio: datos biométricos

2.- OBJETO ESPECÍFICO DE ESTUDIOS		
RGPD	LOPDPGDD	LFPDPPP
. Artículo 9. Tratamiento de categorías especiales de datos personales 1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.	Artículo 9. Categorías especiales de datos 1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.(…) 2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.(…)	Artículo 3 Para los efectos de esta Ley, se entenderá por: (…) V. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. VI. 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.

[51] "Considerando lo siguiente (…) (10) El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito." RGPD p. 2 *https://www.boe.es/doue/2016/119/L00001-00088.pdf*

Nota: Esta tabla muestra cómo el término de datos biométricos se menciona y reconoce en Europa mientras que en México no se hace mención a ello. *Elaboración propia*

Cabe destacar que precisamente en este objeto específico de estudio, se denota claramente que en la ley mexicana no se aduce siquiera al término de datos biométricos bajo la condición de datos sensibles, algo que en las leyes de Europa si se indica claramente, incluso se le define como tal, siendo el contenido del artículo 4 número 14)[52] el que lo establece, para definir las responsabilidades que surgirían del tratamiento ilegal de este tipo de datos personales, y que incluso son clasificados como una categoría especial de tratamiento, siendo lo que arroja este estudio al realizar este análisis comparativo. En México, si bien el concepto de "datos que afecten la esfera más íntima del titular" refiere por interpretación a cualquier dato personal de entre ellos los datos biométricos no se le menciona, no se le define, ni mucho menos se le reconoce como una categoría especial.

2.4.4 Ámbitos de aplicación

El ámbito de aplicación de una norma jurídica debe estar claramente delimitado, debido a que al regular relaciones entre personas físicas o morales, ya sean de carácter público o privado, la coercitividad de la ley debe ser cumplida. También debe especificar su área de aplicación, tal como material y territorial. Tanto en la Unión Europea como en el reino español, el ámbito de aplicación refiere a la persona pública o privada que realiza cierto tratamiento de datos personales, incluyendo aquellos que sean tratados dentro o fuera de la Unión Europea, además de los aplicables en la legislación española por normas de Derecho Internacional, siendo precisamente el área de aplicación de forma material y territorial.

En relación con la LFPDPPP, queda especificado que es aplicable a las personas físicas y morales particulares, haciendo excepción a las sociedades de información crediticia y a las personas físicas que posean datos personales sin ninguna pretensión económica. Por otro lado, la legislación mexicana hace especificación en delimitar el tratamiento hecho tanto por personas y/o entidades públicas, así como privadas, siendo una separación clara referida en la otra ley

[52] 14) «datos biométricos»: 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 confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos; RGPD p. 34 *https://www.boe.es/doue/2016/119/L00001-00088.pdf*

mexicana de protección de datos, denominada LGPDPPSO código que le precedió al estudiado en esta investigación, y que no se dio, sino hasta el 26 de enero del 2017, siendo precisamente los Sujetos Obligados las personas y/o entidades públicas gubernamentales a las que les sea aplicable el contenido de la ley citada.

La diferencia entre esta comparativa radica en que la ley de Europa, incluyendo la ley española, es aplicable a los operadores de datos que ejercen tanto en el área pública como en el privado en el mismo código, ya sea en el ámbito de aplicación material como extraterritorial, mientras que en la regulación mexicana, si bien es aplicable en ambos ámbitos, se hace y se regula de forma separada, atendiendo a los sujetos que intervienen en el tratamiento, ya sea por sujetos obligados del sector público, o los particulares quienes son por el sector privado, siendo la LFPDPPP objeto del presente estudio, y la que finalmente establezca las sanciones respectivas que se den por el tratamiento hecho con la intención de un fin de lucro por parte del sector privado, haciendo excepción como ya se ha mencionado, al hecho por las sociedades de información crediticia.

Los sujetos que intervienen y que se involucran en el tratamiento de datos, son quienes finalmente se les aplicarán las sanciones establecidas en cada ley, y por lo tanto, vendría siendo el ámbito directo de aplicación, siendo los siguientes articulados los que definan a los sujetos que intervienen, los cuales son:

Tabla 2.3

Ámbito de aplicación: sujetos que intervienen

3.- ÁMBITO DE APLICACIÓN		
RGPD	LOPDPGDD	LFPDPPP
. Artículo 4. Definiciones A efectos del presente Reglamento se entenderá por: (…) 7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios	Artículo 33. Encargado del tratamiento 1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.	LFPDPPP. Artículo 2 y 3 Artículo 2.- Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de: I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y

del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros; 8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;	5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.	II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial. Artículo 3.- Para los efectos de esta Ley, se entenderá por: (…) IX. Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable. (…) XIV. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Nota: Esta comparativa señala quienes son los sujetos sobre quienes les es aplicable las leyes estudiadas. *Elaboración propia*

2.4.5 Consentimiento

Las condiciones de licitud de tratamiento, o comúnmente mencionado como consentimiento, es un elemento importante que debe ser respetado al momento de realizar un tratamiento de datos personales, debido a que es la manifestación expresa de la voluntad del titular para otorgarlos, y debe estar debidamente consentida, expresada y manifestada, y que de no tenerse ese consentimiento, no podría efectuarse entonces la transferencia de información personal que el responsable hace, y menos si se tratase de datos sensibles, como es el caso de los datos biométricos, ya que en las legislaciones europeas no es suficiente con el consentimiento expreso, sino que debe ir acompañado de requerimientos que las leyes señala, y por lo tanto se estaría incurriendo en una violación a lo establecido en la ley. Las leyes estudiadas señalan que es indispensable el consentimiento del titular sobre todo enfocado en los datos personales sensibles o especialmente protegidos. Las leyes de Europa, España y México son similares respecto al consentimiento, que a continuación se muestra en la siguiente tabla.

Tabla 2.4

Consentimiento de tratamiento de datos personales

4.- ÁMBITO DE APLICACIÓN		
RGPD	LOPDPGDD	LFPDPPP
Artículo 4. Definiciones: (…) 11) 11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen; Artículo 7. Condiciones para el consentimiento 1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento. 3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de	Artículo 6. Tratamiento basado en el consentimiento del afectado. 1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. 2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas. 3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual. Artículo 7. Consentimiento de los menores de edad. 1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el	Artículo 3. Para los efectos de esta Ley, se entenderá por:(…) IV. Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos. Artículo 8.- 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. Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente Ley.

4.- ÁMBITO DE APLICACIÓN		
RGPD	LOPDPGDD	LFPDPPP
ello. Será tan fácil retirar el consentimiento como darlo. 4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.	consentimiento para el tratamiento. 2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.	

Nota: Esta tabla muestra las formas de conceptualizar el consentimiento de datos personales por parte de cada ordenamiento jurídico. *Elaboración propia*

2.4.6 Aviso de privacidad

Un aspecto relevante en este estudio el cual es necesario mencionar, va en torno al aviso de privacidad, que tiene por objeto el informar las causas y los fines por los cuales se recolectan los datos personales, para dar certeza sobre lo autorizado y en su caso el tratamiento hecho bajo su consentimiento. En el RGPD de la Unión Europea si bien ni siquiera menciona la frase “aviso de privacidad” es sabido que en los numerales 12, 13 y 14 es donde se hace referencia a esta obligación, siendo el capítulo III conocido como derechos del interesado, donde se explica cómo “Transparencia y modalidades”. El artículo 13 se identifica como *información que deberá facilitarse cuando los datos personales se obtengan del interesado,* como el derecho de la recogida de datos para anunciar cualquier actividad relacionada con su información personal. Por otro lado, en España se identifica como Transparencia e información a la figura jurídica equiparable al aviso de privacidad de México.

En México se le denomina como aviso de privacidad, al anuncio que debe hacer el particular de informar a los titulares de los datos, el tipo de información que se recaba de ellos y los motivos de tratamiento que se les dará a los datos.

Las legislaciones en cita destacan una serie de condiciones para darle a conocer al particular los motivos del tratamiento, además de que el interesado otorgue su consentimiento claramente. La diferencia principal entre estas legislaciones es que en Europa y España se le denomina en general como Transparencia e información, siendo el derecho de la recogida de datos, mientras que en México es establecido como aviso de privacidad, para notificar a los titulares sobre quien recaba su información y saber con qué fines se realiza un tratamiento, pero que al final no afecta ni altera este derecho tan importante de las personas. Lo anterior se corrobora en la siguiente tabla:

Tabla 2.5

Aviso de privacidad o derechos del interesado

5.- AVISO DE PRIVACIDAD		
RGPD	LOPDPGDD	LFPDPPP
Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado 1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.	LOPDPGDD. Artículo 11 Artículo 11. Transparencia e información al afectado. 1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. 2. La información básica a la que se refiere el apartado anterior deberá contener, al menos: a) La identidad del responsable del tratamiento y de su representante, en su caso. b) La finalidad del tratamiento. c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.(…)	Artículo 3.- Para los efectos de esta Ley, se entenderá por: I. Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley.

Nota: Esta tabla demuestra las diversas formas en se refiere al aviso de privacidad las leyes estudiadas. *Elaboración propia*

2.4.7 Principio de Confidencialidad

Un principio importante que no debe pasar desapercibido es el principio de confidencialidad, que más que un principio, se reconoce como el deber del responsable del tratamiento de acuerdo a la dicho en la Guía para Titulares de Datos Personales, donde se menciona que el derecho a la protección de datos personales se ejerce a través de ocho principios y dos deberes, los cuales se traducen en tareas que se asignan obligatoriamente a los responsables del tratamiento, y en derechos de los titulares[53]. En relación a los principios, son conocidos como los siguientes:

1. Licitud
2. Lealtad
3. Información
4. Consentimiento
5. Finalidad
6. Proporcionalidad
7. Calidad
8. Responsabilidad

Por otro lado, el manual citado refiere a los deberes como:

1. Seguridad
2. Confidencialidad

Al ser entendida la confidencialidad como un deber, refuerza el entendido de que la información o datos en cuestión deben estar salvaguardados, y que sean sólo transmitidos a los sujetos de la relación, o bien, a quienes se les dio autorización; este principio restringe ciertas libertades del responsable del tratamiento, con el objetivo que el manejo de estos datos se hagan con un sentido de ética digital tal como lo dice Jorge Balladares[54] debido a que en esta época de avance tecnológico, es de suma

[53] Guía para Titulares de los Datos Personales, Volumen 2, p. 6 *https://www.cinvestav.mx/Portals/0/sitedocs/tyr/GuiaTitulares-02_PDF.pdf*

[54] Jorge Balladares “una ética digital para las nuevas generaciones digitales” Pontificia Universidad Católica del Ecuador, Dirección de Pastoral Universitaria, Área de Ética. Quito, Ecuador 2017 *https://www.researchgate.net/publication/316748846_Una_etica_digital_para_las_nuevas_generaciones_digitales*

importancia el tener presente este nuevo estilo de la ética, debido a que, a decir de este autor, la "ética digital contribuye a una explicación y comprensión de la relación del ser humano con la tecnología, e invita a considerar la urgencia de que los diferentes estilos de vida de las nuevas generaciones requiere de referentes éticos para su actuar y convivir en la sociedad digital."[55]

Tanto la ley de Europa como la ley española tienen similitud en cuanto al principio de confidencialidad, además que, de forma implícita, por el reconocimiento de una categoría especial de tratamiento de datos, se incluiría el deber del secreto de los datos biométricos, estableciéndose como una obligación dirigida hacia el responsable de recabar información y de garantizar el cumplimiento de este deber para que pueda prevalecer, algo que, por el contrario, al no estar siquiera mencionado o reconocido en alguna ley, como lo es en el caso de la LFPDPPP en relación a los datos biométricos, no se puede garantizar del todo el principio de confidencialidad aducido en este rubro en materia de datos biométricos. En la siguiente tabla se hace la comparativa aludida en párrafos recientes.

Tabla 2.6

El principio de confidencialidad

6.- AVISO DE PRIVACIDAD		
RGPD	LOPDPGDD	LFPDPPP
Artículo 5. Principios relativos al tratamiento 1. Los datos personales serán: (…) f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).	Artículo 5. Deber de confidencialidad. 1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679. 2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable. 3. Las obligaciones establecidas en los apartados anteriores se	Artículo 21.- El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

[55] Op. Cit. p. 546

6.- AVISO DE PRIVACIDAD		
RGPD	LOPDPGDD	LFPDPPP
	mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.	

Nota: La tabla contiene referencias legales en torno al principio de confidencialidad de las leyes estudiadas. *Elaboración propia*

2.4.8 Transferencia de datos

La transferencia de datos personales a terceros es una situación delicada y cada vez más común en la globalización digital, debido a que se considera una violación a los derechos del titular cuando se realiza cierto tratamiento sin el consentimiento del interesado por empresas terceras que de alguna forma no obtuvieron dicho consentimiento, y por lo tanto se realiza con fines distintos a los establecidos en la recolección original, lo cual vulnera la privacidad y la intimidad de la información de las personas.

Como ya se adujo en el aviso de privacidad, el responsable del tratamiento debe informar todo trabajo con los datos biométricos, sobre todo por el hecho de saber quién tiene la posesión de los mismos. La transmisión de datos a terceros ya sean nacionales o extranjeros deben ser notificados al titular, así como el tratamiento que llevará a cabo el sujeto responsable, viéndose obligado a cumplir con los lineamientos respectivos. La diferencia radica en los términos utilizados en las leyes estudiadas, ya que en México la transferencia de datos es la acción de otorgar información personal a otros particulares, mientras que en España esta actividad se le llama comunicación de datos.

Pero en la presente comparativa, se llega a la conclusión, que en el caso mexicano, al igual que en el principio de confidencialidad estudiado previamente, aunque este referido la transferencia de datos, no puede garantizarse del todo su cumplimiento, debido a que en la codificación mexicana, si bien es cierto reconoce los datos sensibles, dentro de los mismos ni siquiera se identifican o especifican los datos biométricos.

Tabla 2.7

Transferencia de datos

7.- TRANSFERENCIA DE DATOS		
RGPD	LOPDPGDD	LFPDPPP
Artículo 44. Principio general de las transferencias Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo (…) Artículo 45. Transferencias basadas en una decisión de adecuación 1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica. (…)	LOPDPGDD. Artículo 40 Artículo 40. Régimen de las transferencias internacionales de datos. Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias. En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.	Artículo 3. Para los efectos de esta ley, se entenderá por: (…) XIX. Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento. Artículo 36.- Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

Nota: Esta tabla identifica los artículos que refieren a la transferencia a terceros nacionales o extranjeros. *Elaboración propia*

2.4.9 Derechos de las personas

Un medio legal a favor del titular de datos personales que le permite ejercer su derecho a la autodeterminación informativa como un escudo protector de los derechos a la privacidad y a la intimidad frente a las empresas particulares que den tratamiento a los mismos, son los ya mencionados derechos ARCO: de acceso, rectificación,

cancelación y oposición, además de incluir algunos otros en la Unión Europea. En este contexto, la derogada Ley Orgánica 15/1999 de Protección de Datos de carácter personal fue reforzada por el RGPD. Desde el inicio de su vigencia, los anteriores derechos ARCO fueron ampliados para salvaguardar todavía más la invulnerabilidad de los datos personales. Estos derechos se pueden identificar ahora en el RGPD cómo ARCO-POL, siendo siete derechos exigibles ante la ley tanto en competencia de la Unión Europea como en España por la interrelación que tienen por su derecho comunitario, los cuales son: acceso, rectificación, supresión (cancelación), oposición, portabilidad, olvido y limitación del tratamiento.

Por otro lado, en México sólo se reconocen los derechos ARCO como mecanismos exigibles, siendo garantías que de alguna forma son similares con los ordenamientos jurídicos europeos, las cuales finalmente comparten el mismo objetivo, pero sigue quedando pendiente la reforma respectiva en relación a incluir los derechos como la portabilidad, el derecho al olvido y la limitación del tratamiento, sobre todo por el hecho de extender el espectro jurídico de defensa de datos personales en relación con los datos biométricos en el momento que se reconozcan y delimiten claramente en las leyes mexicanas. Lo anterior se demuestra en la tabla No. 8

Tabla 2.8

Derechos ARCO y relativos

8.- Derechos ARCO y relativos		
RGPD	LOPDPGDD	LFPDPPP
Artículos: 15, 16, 17, 18, 19, 20, 21 y 22 Artículo 15. Derecho de acceso al interesado 1.El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información: (…) Artículo 16. Derecho de rectificación	Artículos del 12, 13, 14 ,16 16, 17 y 18 Artículo 12. Disposiciones generales sobre ejercicio de los derechos. 1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario. 2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden.	Artículos 22, 23, 24, 25, 26 y 27 Artículo 22.- Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.

8.- Derechos ARCO y relativos		
RGPD	LOPDPGDD	LFPDPPP
El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. (…) Artículo 17. Derecho de supresión («el derecho al olvido») 1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: (…) Artículo 18. Derecho a la limitación del tratamiento 1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: (…) Artículo 19. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento Artículo 20. Derecho a la portabilidad de los datos 1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: (…) Artículo 21. Derecho de oposición	Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio. 3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule. (…) Artículo 13. Derecho de acceso. 1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679. Artículo 14. Derecho de rectificación. Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento. Artículo 15. Derecho de supresión. 1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679. 2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir	Artículo 23.- Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento. Artículo 24.- El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos. Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales. La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia. (…) Artículo 27.- 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.

8.- Derechos ARCO y relativos		
RGPD	LOPDPGDD	LFPDPPP
1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. (…) Artículo 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles 1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.	tratamientos futuros para fines de mercadotecnia directa. Artículo 16. Derecho a la limitación del tratamiento. 1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679. 2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable. Artículo 17. Derecho a la portabilidad. El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679. Artículo 18. Derecho de oposición. El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.	

Nota: Los derechos ARCO y relativos de las personas que se reconocen en los ordenamientos jurídicos estudiados se describen en la tabla anterior. *Elaboración propia*

2.4.10 Autoridades competentes para la protección de datos biométricos

La obligación del Estado a través de su elemento del poder, es asignar las autoridades públicas pertinentes que hagan valer los derechos reconocidos en la constitución, delimitando su competencia y objetivos acorde a los derechos de protección de datos personales. En relación con Europa, España y México, cabe mencionar que cada uno de éstos cuenta con sus propias autoridades de protección de datos, debidamente delimitadas sus funciones y sus jurisdicciones territoriales.

Los países de la Unión Europea han creado organismos responsables de proteger los datos personales, tal como establece el artículo 8, apartado 3, de la Carta de los Derechos Fundamentales de la Unión Europea[56], siendo precisamente el Comité Europeo de Protección de Datos la autoridad de Europa el que tome responsabilidad sobre el tema. Por otro lado, En España, tal como ya se ha mencionado, se distingue la AEPD, mientras que a nivel autonómico existen autoridades respectivas para cada entidad. En México, claramente se distingue al INAI como el organismo garante de protección de datos, existiendo de igual forma que en España, una autoridad local para la protección de datos personales en cada entidad federativa.

Las autoridades encargadas de observar que los datos personales sean respetados es otro factor importante dentro de este estudio de derecho comparado, para verificar si es que cuentan con organismos facultados para proteger los derechos a la intimidad y la privacidad de las personas, cuestiones que están en juego dentro del tratamiento de datos biométricos, y así no sean violentados sus derechos al momento que cierta empresa u organización realice ciertos tipos de tratamiento. Lo anteriormente expuesto, puede corroborarse en la siguiente tabla:

Tabla 2.9

Autoridades competentes para la protección de datos biométricos

9.- Autoridades competentes		
RGPD	LOPDPGDD	LFPDPPP
Artículo 68. Comité Europeo de Protección de Datos 1. Se crea el Comité Europeo de Protección de Datos («Comité»), como organismo de la Unión, que gozará de personalidad jurídica. 2. El Comité estará representado por su presidente. 3. El Comité estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de	Artículo 44. Disposiciones generales. 1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones. Su	Artículo 38.- El Instituto, para efectos de esta Ley, tendrá por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos

[56] Autoridades nacionales de protección de datos. *https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es*

9.- Autoridades competentes		
RGPD	LOPDPGDD	LFPDPPP
Datos o sus representantes respectivos. 4. Cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro. 5. La Comisión tendrá derecho a participar en las actividades y reuniones del Comité, sin derecho a voto. La Comisión designará un representante. El presidente del Comité comunicará a la Comisión las actividades del Comité. 6. En los casos a que se refiere el artículo 65, el Supervisor Europeo de Protección de Datos sólo tendrá derecho a voto en las decisiones relativas a los principios y normas aplicables a las instituciones, órganos y organismos de la Unión que correspondan en cuanto al fondo a las contempladas en el presente Reglamento.	denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente». Se relaciona con el Gobierno a través del Ministerio de Justicia. 2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos. 3. La Agencia Española de Protección de Datos y el Consejo General del Poder Judicial colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.	regulados por este ordenamiento. Artículo 39.- El Instituto tiene las siguientes atribuciones: I. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación; II. Interpretar en el ámbito administrativo la presente Ley; III. Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley; IV. Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables de esta Ley, para efectos de su funcionamiento y operación; V. Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable; (…) XII. Las demás que le confieran esta Ley y demás ordenamientos aplicables.

Nota: En la tabla se identifican las autoridades competentes para velar por la protección de los datos biométricos. *Elaboración propia*

2.4.11 Infracciones y sanciones

La necesidad de adoptar medidas fundamentales para evitar la fuga de los datos por las empresas es tal vez la preocupación más vital que se debería considerar al momento de ponderarlo con el derecho a la privacidad y protección de datos

personales, además de las faltas deliberadas que cometa el operador del tratamiento, específicamente dentro del manejo de datos sensibles del titular, siendo precisamente la importancia de que se cumpla la norma jurídica, y universalizar una praxis segura en todas las empresas, tal como el *compliance*[57] o algún otro medio. Por lo tanto, se ha identificado que las infracciones que se encuentran en las leyes estudiadas, deben contar con una determinada sanción respecto al tipo de falta que cometió el operador del tratamiento, en relación con el manejo de datos del titular, aspectos encontrados en las tres leyes comparadas.

2.4.11.1 Las infracciones en las leyes de Europa

Es importante identificar que los responsables del tratamiento de datos son las compañías o empresas que tienen su domicilio fiscal en la Unión Europea o bien, realicen tratamiento de datos personales a ciudadanos europeos, los cuales, de acuerdo a los ámbitos de aplicación del RGPD, serían el ámbito material y territorial, y que precisamente si violentan los lineamientos europeos y las leyes específicas de los países de los interesados, serían merecedores de las infracciones de las leyes. Al mismo tiempo, se les exige respetar el principio de responsabilidad activa de las empresas, que refiere a que las compañías se vuelvan proactivas en cuanto a la obligación y la responsabilidad de llevar a cabo su propia gestión de riesgo[58]

Cada Estado Miembro dispone de una o varias autoridades de control que se encargan de velar por la aplicación y cumplimiento del RGPD. Entre las diferentes competencias que el Reglamento les atribuye se encuentra el poder correctivo, que incluye la facultad de sancionar aquellas actividades que infrinjan lo dispuesto en el RGPD.

Las clasificaciones de infracciones en Europa son muy claras en definir los actos que van en contra de lo regulado, así como las omisiones realizadas, señalando las acciones con una menor repercusión por un lado o un gran impacto por otro.

[57] sirve como un guía de prevención y cumplimiento de leyes, que en conjunto con códigos éticos y de buenas prácticas, puede ayudar a las organizaciones a identificar y clasificar los riesgos operativos y legales a los que se enfrentan día con día. Su objetivo es aplicar programas que inciten actuaciones respetuosas con la ley, derivadas de los trabajadores o de la propia organización, para así evitar la responsabilidad penal como personas jurídicas.

[58] Las sanciones más comunes por incumplimiento del RGPD en 2021 en Europa y España *https://nymiz.com/es/blog/proteccion-de-datos/las-sanciones-mas-comunes-por-incumplimiento-del-rgpd-en-2021-en-europa-y-espana/*

Actualmente, las infracciones por protección de datos en el RGPD se dividen en 2 categorías: sanciones graves y sanciones muy graves, no objetando que dentro de las regulaciones de los países miembros pudieran clasificar las infracciones como no graves también.

Las Infracciones muy graves del RGPD son aquellas que suponen un incumplimiento sustancial del tratamiento, teniendo como plazo de prescripción tres años, y están relacionadas con:

1. Una omisión del deber de correcta información al afectado.
2. El uso de los datos para una finalidad distinta a la acordada.
3. La exigencia de un pago por acceder a los datos propios almacenados.
4. Una transferencia internacional de información sin garantías.

En estos supuestos se establece una sanción con multas administrativas que pueden alcanzar los 20 millones de euros o, en el caso de una empresa, un importe equivalente al 4% de la facturación anual.

Las infracciones graves del RGPD son las que suponen una vulneración sustancial del tratamiento, tienen un plazo de prescripción de 2 años y están relacionadas con:

Los datos de un menor recabados sin consentimiento.

El incumplimiento de nombrar un responsable o encargado de tratamiento de datos.

La ausencia de medidas técnicas y organizativas necesarias para una protección de datos auténtica.

En este caso se sancionará con multas administrativas que pueden llegar a un importe máximo del 2% de la facturación anual de la empresa.

2.4.11.2 Infracciones y sanciones en España

En supuestos de incumplimiento de la LOPDGDD se puede interponer una denuncia de protección de datos ante la AEPD, que es la autoridad de control del cumplimiento de esta normativa en España. Las sanciones por no cumplir la ley de protección de datos pueden alcanzar hasta los 20 millones de euros o el 4% del

volumen de facturación anual. Las infracciones se dividen en leves, graves y muy graves.

La cuantía de las sanciones por protección de datos que la LOPDGDD impone, se valora según los derechos personales afectados, los beneficios obtenidos, reincidencia, intencionalidad y cualquier circunstancia que sea relevante para determinar la culpabilidad.

2.4.11.3 Las infracciones y sanciones en México

En lo que respecta a la legislación mexicana, la LFPDPPP se menciona los casos en que se puede llegar a infraccionar al responsable del tratamiento. La normativa mexicana no tiene una clasificación de infracciones jerarquizada como en Europa, simplemente contempla las acciones perjudiciales a la información personal y los actos omisos efectuados, sobre todo ante la solicitud de derechos ARCO de los titulares de los datos personales. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, será acreedor de una sanción de 100 a 160,000 veces el valor de la UMA. Si se declara que no existen tales datos personales en las base de datos y existe un rastro de que si, se hace uno inmediatamente acreedor de esa sanción.

Cabe mencionar que también son merecedores de sanciones los particulares que se encuadren en el contenido del artículo 64 de la LFPDPPP sobre omitir colocar un aviso de privacidad en los medios que disponga el particular. Cuando resulten afectados los derechos de los titulares, y no cumplir con el apercibimiento de la autoridad, será acreedor de una multa de 200 a 320,000 veces el valor de la UMA. En caso de que se venda o trasmita los datos para otros fines o en caso de que un usuario haya solicitado el no uso de sus datos y aun aparezcan, será acreedor de una multa de que irá de 100 a 320,000 veces el valor de la UMA. En caso de que de manera reiterada persistan las infracciones citadas, tal como lo dice el artículo 64 fracción IV, en tratándose de infracciones cometidas en el tratamiento de datos sensibles, siendo considerados como parte de éstos los datos biométricos, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.[59]

[59] Artículo 64.- Las infracciones a la presente Ley serán sancionadas por el Instituto con: (…)
IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones

Por otro lado, no olvidar lo establecido en el Capítulo XI, que establece sanciones penales por el tratamiento indebido de datos, precisamente denominado “De los Delitos en Materia del Tratamiento Indebido de Datos Personales” el cual abarca del artículo 67 al 69 de la ley en comento, que a la par dice:

- Artículo 67.- Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.
- Artículo 68.- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.
- Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

Es importante mencionar que el tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Se debe cancelar aquellos datos que han dejado de ser necesarios para el cumplimiento de las finalidades previstas en los avisos de privacidad y se debe evitar solicitar datos personales innecesarios, ya que entre más información se tenga, es mayor la responsabilidad y el riesgo de hacer mal uso de ella

2.4.11.4 Comparativa de las infracciones y sanciones en Europa, España y México

Es importante señalar que una de las principales diferencias entre las legislaciones, es que, mientras en Europa y España se realiza una clasificación de las infracciones, en la legislación mexicana no contempla dicha jerarquización. Lo anterior indica que en Europa suele ser más estricto en relación a las violaciones derivadas de un tratamiento de datos personales que aquellas reconocidas en la legislación mexicana. De acuerdo a la siguiente tabla comparativa, se muestran los preceptos legales del RGPD más sancionados, así como la postura de las leyes españolas y mexicanas.

podrán incrementarse hasta por dos veces, los montos establecidos. *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*

Tabla 2.10

Infracciones y sanciones en las leyes comparadas

10.- Infracciones y sanciones		
RGPD	LOPDPGDD	LFPDPPP
Artículo 5, 6 y 32, 83, 84 Artículo 5. Principios relativos al tratamiento (..) 2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»). Artículo 6. Licitud del tratamiento (…) 4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento (…) Artículo 83. Condiciones generales para la imposición de multas administrativas 1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias. 2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el	Artículos 3, 9, 10, 27, 28 y 70, a 78. Artículo 3. Datos de las personas fallecidas Articulo 9. Categorías especiales de datos Artículo 10. Tratamiento de datos de naturaleza penal Artículo 27. Tratamiento de datos relativos a infracciones y sanciones administrativas Artículo 28. Obligaciones generales y responsable del tratamiento Artículo 70. Sujetos responsables Artículo 71. Infracciones Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica. Artículo 72. Infracciones consideradas muy graves. Artículo 73. Infracciones consideradas graves. Artículo 74. Infracciones consideradas leves Artículo 76. Sanciones y medidas correctivas Artículo 77. Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento Artículo 78. Prescripción de las sanciones	Artículos 63, 64, 65, 66, 67, 68 y 69 Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable: I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley; II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales; III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable; (…) Artículo 64.- Las infracciones a la presente Ley serán sancionadas por el Instituto con (…) II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior; III. Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior, y IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional

10.- Infracciones y sanciones		
RGPD	LOPDPGDD	LFPDPPP
artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta(…) 4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía: (…) Artículo 84. Sanciones 1. Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias. (…)		que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos. Artículo 65.- El Instituto fundará y motivará sus resoluciones, considerando (…) Artículo 66.- Las sanciones que se señalan en este Capítulo se impondrán sin perjuicio de la responsabilidad civil o penal que resulte. Artículo 67.- Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia. Artículo 68.- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos. Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

Nota: En la tabla anterior se describen las sanciones e infracciones que establecen estos códigos.
Elaboración propia

De lo anterior se desprende que en México es necesario fijar una clasificación de infracciones para que el operador de sistemas biométricos tenga bien sabido las consecuencias a las que se puede enfrentar.

2.5 Conclusiones preliminares del capítulo II

Del estudio anterior del capítulo II se advierte que los sistemas jurídicos a los que pertenecen los países comparados y la U.E son compatibles, y por lo tanto viables de tomarse como ejemplo o referencia, al momento de actualizar y reformar el contenido de una ley. Es por esto que, de los once puntos colisionados de las leyes de protección de datos contrastadas, se puede deducir que tienen similitud en la mayoría de ellos, pero claramente las legislaciones Europeas son mucho más amplias, actualizadas y completas en contraste con la ley mexicana que, si bien fue innovadora en el momento de su promulgación ya desde hace diez años, ha quedado muy corta al momento de confrontar la realidad del avance tecnológico y digital que sobrepasa el contenido de la ley rápidamente, y por ello la importancia de mantenerse actualizado en estos temas, para así positivizarlo a través de reformas y actualizaciones del contenido de las mismas, adecuándolas a la realidad, e incluso adelantándose a ella para regular lo que advertida o inadvertidamente pueda llegar.

Por supuesto que de los once puntos comparados, existen datos notablemente sobresalientes, de los cuales se resaltarán los siguientes, tales como: el objeto específico de estudio de los datos biométricos, donde claramente las leyes Europeas lo definen y prohíben su tratamiento en ciertos casos, mientras que en México la ley simplemente lo aduce indirectamente, y no establece ninguna categoría especial de tratamiento o sanción específica por su manejo; el principio del consentimiento, donde la ley mexicana aún tiene la vaguedad de reconocer el consentimiento tácito y los particulares se aprovechen de este punto para recopilar datos; o el derecho que las leyes reconocen a las personas para que hagan frente a los particulares que realicen un tratamiento ilegal de sus datos, donde como se ha visto, las leyes europeas garantizan tres derechos más que los derechos ARCO, tales como el derecho a la portabilidad, el derecho al olvido y el derecho de limitación del tratamiento de datos.

Otros resultados importantes que salieron a la luz derivado de la comparativa de leyes, refiere a las autoridades especializadas en protección de datos de Europa y España, donde tienen muy bien especificadas sus funciones, cuestión que en México, si bien el INAI atiende asuntos de protección de datos, también es cierto que atiende asuntos de transparencia y acceso a la información pública gubernamental, circunstancias que demuestran que no tiene un órgano especializado en privacidad y

protección de datos que pueda exponer, sostener y establecer posturas en la materia, sin demeritar los esfuerzos que se han hecho en el INAI y en el Sistema Nacional de Transparencia y sus órganos como la Comisión de Protección de Datos Personales, ya que en este caso, los asuntos de protección de datos son remitidos al INAI y no a la Comisión en comento por tener otras funciones.

Los resultados del contraste de las infracciones interpuestas al tratamiento de datos sensibles son muy variadas. Mientras que en Europa y España se sanciona con grandes cuantías algún indebido tratamiento de datos, sobre todo los especialmente sensibles como lo son los datos biométricos, en México aún es muy genérica su sanción económica, y deja un tanto ambiguo la sanción aplicable en caso de datos especialmente sensibles como lo son los datos biométricos.

Sin duda alguna es de suma importancia el reconocimiento de los derechos digitales que se hizo en España, ya que en México aún no se ha hecho mención al respecto. Estas potestades de las personas son de suma importancia, ya que el avance tecnológico y digital siempre sobrepasa la realidad legal, y por lo tanto su debido reconocimiento, ayudaría mucho a reforzar la protección de datos especialmente sensibles tales como los datos biométricos.

Por lo tanto, de entre estos y muchos otros resultados más, se entiende que es viable resaltar los puntos comparados de acuerdo a la prueba de funcionalidad propuesta en la macrocomparación para determinar más específicamente los datos arrojados de las leyes estudiadas.

CAPÍTULO III. ESTRUCTURACIÓN DE LOS RESULTADOS ARROJADOS POR EL ESTUDIO COMPARATIVO ENTRE EL FACTOR NEUTRAL Y LOS DATOS BIOMÉTRICOS

De la investigación realizada se puede advertir que si bien los resultados de la colisión de las leyes estudiadas arrojan factores importantes, de acuerdo a la prueba de funcionalidad propuesta por Adrián Mancera Cota, primeramente debe identificarse y determinarse si existe la viabilidad y funcionalidad de los sistemas jurídicos en comparación, cuestiones que una vez analizadas en el capítulo II son claramente compatibles entre los sistemas jurídicos estudiados y por lo tanto, se pueden importar en el sistema jurídico mexicano. Por consiguiente, queda comprobada la factibilidad de adoptar una solución extranjera por dos razones: la primera debido a que el resultado de la aplicación de la regulación de datos personales es evidentemente satisfactorio en los países de origen como es la Unión Europea y España, y la segunda, podría funcionar en el país donde se propone su implantación, como lo es México.

3.1 Resultados arrojados por el estudio comparativo

Se afirma que el tratamiento de datos biométricos está regulado en el RGPD y por lo tanto en las leyes de los países miembros de la Unión Europea, como es el caso de España y su LOPDGDD. Cuestión contraria a la situación de México en este rubro, donde se comprueba parcialmente la hipótesis de que, si bien su falta de reconocimiento no entorpece su protección, es evidentemente que existe una falta de positivización de los datos biométricos en las leyes pertinentes. Aunque los datos sensibles sean reconocidos en la LFPDPPP, su mención no garantiza que se protejan los datos biométricos, frente al tratamiento que realicen ciertas empresas u organizaciones en México o diversas partes del mundo, sobre todo aprovechándose del consentimiento tácito aún reconocido en México y algunos otros factores que se mencionarán posteriormente.

El factor neutral de datos personales, permitió que se mantuviera una línea clara sobre la cual se pudiera acercar al estudio e identificación de las categorías subsecuentes como son los datos sensibles. En este punto, el RGPD denota que si bien los datos biométricos se correlacionan con los datos sensibles, éstos vienen siendo una categoría especial de tratamiento, el cual se reconoce como tal junto con los datos genéticos o datos de salud; cuestión diversa en México, que si bien se

reconocen los datos sensibles como las fibras más privadas de los datos personales, destaca por la ausencia de definición de datos biométricos, no solamente en la LFPDPPP o en la LGPDPPSO, sino en leyes u organismos involucrados con la identidad personal para fines diversos, tal como la Ley General de Población que no contaba con estas actualizaciones, pero que actualmente existe una iniciativa con proyecto de decreto para dar la relevancia necesaria a los datos biométricos como herramienta para identificar a los mexicanos[60]; o el padrón electoral del INE a través del Reglamento del Instituto Nacional Electoral en materia de Protección de datos personales en el cual se pudiera definir, entre otros.

Se han cumplido los dos objetivos específicos, tal como identificar la naturaleza de los datos biométricos a nivel académico y legal, así como emprender el estudio comparativo de las variables, como son los reglamentos y leyes de protección de datos personales de Europa, España y México en relación a la protección de datos biométricos, a través de diversos métodos de estudio, tal como el analítico, comparativo, deductivo y sistemático, cuestión analizada a través de los once puntos contrastados en el capítulo II, donde se utilizó como factor neutral los datos personales, con el objetivo de incluir dentro de este análisis lo relativo a la ley mexicana. Estos objetivos nos han arrojado el objeto del tercer objetivo específico, el cual es estructurar los resultados emitidos por la colisión del RGPD de la Unión Europea, la LOPDPGDD de España, y la LFPDPPP de México, donde se percata que derivado de la comparativa, permite identificar los elementos pendientes de incluirse o reconocerse en la legislación mexicana en materia de datos biométricos.

Para estructurar los resultados arrojados por el estudio comparativo precedido a este capítulo, es necesario retomar brevemente los puntos analizados, desde el marco histórico, conceptual y sistemático hecho en el capítulo I, hasta la comparación de sistemas jurídicos y las leyes estudiadas del capítulo II.

Sin duda la biometría no es un tema nuevo, sino que se remonta a miles de años atrás, y su aprovechamiento ha sido importante y trascendente para la identificación y verificación de la identidad de las personas en muchas culturas originarias. Pero al pasar el tiempo, se fueron perfeccionando las técnicas

[60] Ximena Puente de la Mora "*datos personales y biométricos. la apuesta de México ante las tecnologías de la información"* UMH Sapientiae, 2021 p. 46 *https://www.lamjol.info/index.php/UMH-S/issue/view/1542*

biométricas, llegando al punto de la época digital en la cual se optimizaron dichas tecnologías a través de sistemas especializados en biometría. Dicho funcionamiento de estos sistemas, que disponen de datos para su funcionamiento, deben estar debidamente regulados bajo principios de ética digital, privacidad por diseño y por defecto, y por supuesto por las leyes de protección de datos que emita el país involucrado en esta problemática social. De esta manera es que fue necesario remitirse a la doctrina anglosajona y romanista, para extraer los avances que se han dado en ambos sistemas jurídicos en cuestión de privacidad, intimidad y datos personales, para así reforzar la postura de que los datos biométricos están íntimamente relacionados con estos atributos de la personalidad, y por lo tanto su reconocimiento y protección debe ser reconocida en las leyes de protección de datos.

Por otro lado, diversas leyes de Latinoamérica han tenido avances importantes en este tema y han creado mecanismos y autoridades de protección de datos biométricos, mayormente por motivos de seguridad pública tal como Argentina y Colombia, aspectos que como ya se mencionó en el capítulo I, pueden ser tomados de referencia para la eventual creación de la autoridad especializada en datos biométricos en nuestros país.

En cuanto a la problemática de los particulares y las entidades financieras, es una cuestión que debe ser armonizada de alguna manera por el legislador mexicano, para que las entidades financieras en materia de protección de datos rindan cuentas al Organismo Garante y no a autoridades administrativas, financieras o bursátiles las cuales no tienen especialización en la materia ni mucho menos en temas de derechos humanos, ya que el avance de la época digital está obligando a sistematizar datos tanto a particulares como a entidades financieras, tal como las *fintech* o la banca electrónica, y tarde o temprano, alcanzará a cualquier entidad financiera, debiendo regirse por los lineamientos de la LFPDPPP a razón de establecer el marco legal del bien jurídico tutelado de esta ley, el cual es la autodeterminación informativa.

Por lo que ve a los sistemas jurídicos comparados, es viable y denota unos mecanismos comparativos para resaltar los puntos necesarios y pendientes para que México se ponga a la altura de los estándares internacionales en materia de privacidad y protección de datos personales.

A continuación se muestran diez puntos destacables de la comparativa hecha anteriormente, para plantear la síntesis analítica y conclusión comparativa del presente trabajo:

1. La denominación de las leyes estudiadas no altera el bien jurídico tutelado como lo es la privacidad y la protección de datos personales, aunque al ser la ley española muy específica al incluir los derechos digitales de los interesados, éstos mismos deberían incluirse en la LFPDPPP de México, para garantizar de forma más integral el respeto a los datos biométricos.

2. Los datos personales, como factor neutral entre las leyes estudiadas, fueron identificados y conceptualizados en el primer capítulo de esta tesis, remitiéndose a los avances anglosajones y latinoamericanos en la materia, así como también encontrados en las propias leyes de Europa, España y México, se garantizará una protección de los mismos en lo que respecta al tratamiento. Lo único que diferencia en esta comparativa, es que en la ley mexicana se especifica el tratamiento realizado por particulares, mientras que en leyes europeas refiere indistintamente tanto a públicos como privados.

3. Siendo el objetivo específico de estudio los datos biométricos, el RGPD es el único que los define y reconoce, siendo el artículo 4, número 14 que dice: “14) «datos biométricos»: 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 confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”. La legislación española al dar seguimiento del reglamento, no opta por coartar o extender esta definición, sino que más bien le expande el rango de protección de los mismos, estableciendo el grado de gravedad que implica el realizar un mal tratamiento de las categorías especiales de datos, así como establecer requisitos adicionales relativos a la seguridad y confidencialidad de los mismos. En el caso mexicano, si bien reconoce como categoría especial los datos sensibles, no se define ni mucho menos se reconoce o identifica lo que son los datos biométricos, cuestión importante que se podría complementar.

4. El ámbito de aplicación de las leyes estudiadas son los mismos, en cuanto a que las tres leyes son aplicables tanto en un sentido material como en el territorial,

pero haciendo distinción en el caso mexicano entre sujetos obligados y particulares, aspectos que los ordenamientos europeos no distinguen y por lo tanto les son aplicables en ambos casos. Los sujetos que intervienen son quienes finalmente se les aplicarán las leyes referidas, aspectos que en el caso europeo y mexicano se reconocen como dos figuras legales: el responsable de tratamiento y el encargado de tratamiento, siendo el mismo sentido que se les dé en las leyes referidas.

5. Respecto al consentimiento, al ser la piedra angular para realizar un tratamiento de datos autorizado por el interesado o titular, las leyes estudiadas refieren de alguna forma al mismo sentido, sobre todo en cuanto a identificarlo como la manifestación de una voluntad libre, específica, informada e inequívoca, radicando una diferencia importante en la ley mexicana, la cual, aún reconoce dos tipos, siendo el consentimiento expreso, así como el consentimiento tácito, inconvenientes importantes en éste último, debido a que en el RGPD ya no está reconocido como tal, debido a las arbitrariedades que se pueden cometer al contar con la inacción o el silencio por parte del interesado en cuanto al tratamiento de sus datos, riesgos que siguen latentes en la ley mexicana y que deberían subsanarse.

6. El aviso de privacidad, desde el enfoque europeo, técnicamente lo identifican como “transparencia y modalidades”. En la ley española como “transparencia e información al afectado” mientras que en la ley mexicana se distingue llanamente como “aviso de privacidad”, cuestión que para nada afecta su aplicabilidad, ya que en la práctica precisamente se le conoce de la misma forma en la red internet.

7. En relación al principio de confidencialidad, resulta que los lineamientos legales analizados tienen cierta similitud, en cuanto a que la información o datos en cuestión deben estar salvaguardados con medidas adecuadas, sometiéndose a principios y deberes específicos, y más aún en el caso de datos biométricos por ser considerados datos sensibles; discrepancia que se tiene en la legislación mexicana, ya que si bien reconocen los datos sensibles, no se tiene una definición ni especificación de los datos biométricos y por lo tanto, no se pueda garantizar del todo éste principio en algún momento dado.

8. Las leyes europeas estudiadas coinciden en que la transferencia de datos o comunicación de datos a terceros, ya sean éstos nacionales o extranjeros, previo a su transferencia, debe estar debidamente notificado a los titulares a través del aviso

de privacidad, aspectos que son de suma importancia en la globalización digital, y que en caso de incumplimiento, se apliquen las sanciones respectivas. Siendo la excepción el caso mexicano, que si bien reconoce la transferencia de datos, al hacer falta la categorización de datos biométricos, los titulares podrían quedar en un estado de indefensión frente a las empresas u organizaciones particulares interesadas, sobre todo por el consentimiento tácito aún reconocido en la LFPDPPP.

9. El escudo protector de los derechos a la personalidad, y por lo tanto la privacidad y la intimidad, frente a las empresas particulares que den tratamiento a los mismos, son los ya mencionados derechos ARCO, acrónimo de derechos que siguen vigente en la ley mexicana, pero que en Europa se ha extendido a reconocerse como ARCO-POL, siendo éstos los derechos de acceso, rectificación, supresión (cancelación) y oposición, además de tres más que se reconocen, tal como la portabilidad, el olvido y la limitación del tratamiento, derechos de las personas que quedarían pendientes de incluir en la legislación mexicana.

10. Los países estudiados cuentan con autoridades competentes para garantizar la protección de los derechos a la privacidad y libre autodeterminación informativa, aspectos que salen a relucir al momento de contrastar los artículos específicos de las leyes planteadas.

11. Las infracciones y sanciones que los ordenamientos legales europeos establecen, deberían tomarse como guía para incluirse en la ley mexicana, como por ejemplo la categorización de sanciones graves, o sanciones muy graves que el RGPD manda, ya que la normativa mexicana no tiene una clasificación de infracciones jerarquizada como en Europa, simplemente contempla las acciones perjudiciales a la información personal y los actos omisos efectuados, aspectos que quedarían ambiguos al momento de establecer una sanción adecuada por el mal tratamiento de datos biométricos.

Todos estos puntos podrían ser considerados al momento de reformar la LFPDPPP, donde es de suma importancia el que se actualice en torno a los derechos digitales y por supuesto se incluya la categorización de datos sensibles, siendo parte de estos los datos biométricos, en conjunto con los datos médicos, datos genéticos y los neurodatos estableciendo algún límite a su tratamiento.

3.2 Consideraciones de los puntos contrastados

Las consideraciones que resaltan de los puntos contrastados, ponen de manifiesto las actualizaciones que se puedan hacer en la LFPDPPP en torno al tema de los datos biométricos, y dentro de éstas, sin duda la definición de datos biométricos y su reconocimiento como dato especialmente sensible es de las más importantes, al igual que los tipos de categorización del tratamiento de datos personales, los procesos de tratamiento a gran escala, la extensión de los derechos de las personas, y las infracciones pormenorizadas del tratamiento de datos.

Es una referencia sumamente importante la definición y reconocimiento como datos sensibles la figura de los datos biométricos en el RGPD, aquella que se encuentra en el artículo 4 número 14, y que debería tomarse de ejemplo, e incluso perfeccionarlo y adecuarlo a la realidad mexicana, incluyendo una definición en el artículo 3 de la LFPDPPP y todo lo que eso conlleva en la ley.

En cuanto a los tres tipos de categorización de datos personales, debería incluirse en la ley mexicana las categorías especiales, tales como los relacionados a los datos genéticos, datos biométricos y datos de salud. Una opción puede ser repetir el modelo del RGPD, o bien y por lo menos, incluir dentro de los datos sensibles los datos biométricos expresamente, para no dejar a la interpretación que los biométricos deben tener ese carácter y, por lo tanto, su protección quede reforzada. Por otra parte, tal como el RGPD lo establece debería incluirse también lo referido a definir algunas listas de tipos de tratamientos de datos que requieran evaluación de impacto, sobre todo a tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física[61]

México no es ajeno a los procesos de tratamiento a gran escala de datos biométricos La importancia de esos datos en el ámbito de las transacciones comerciales y de bienes y servicios en general es muy alta, y en esa medida, su

[61] El RGPD dedica la Sección 3 de su capítulo IV “Responsable del tratamiento y encargado del tratamiento” a la Evaluación de Impacto relativa a la protección de datos. En concreto, el apartado 1 del artículo 35 establece, con carácter general, la obligación que tienen los responsables de los tratamientos de datos de realizar una EIPD con carácter previo a la puesta en funcionamiento de tales tratamientos cuando sea probable que éstos por su naturaleza, alcance, contexto o fines entrañen un alto riesgo para los derechos y libertades de las personas físicas, alto riesgo que, según el propio Reglamento, se verá incrementado cuando los tratamientos se realicen utilizando “nuevas tecnologías” p. 1 *https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf*

reconocimiento expreso en la ley sería de mucha ayuda para su blindaje jurídico y así provocar un efecto jurídico particular con ese reconocimiento, donde su utilización se limite a los casos estrictamente necesarios y que su uso vaya siempre acompañado de una justificación plena. Son múltiples las plataformas y aplicaciones que se valen de este tipo de datos para prestar sus servicios ¿está justificado en todos los casos? Para responder a esa pregunta, y como complemento a lo ya señalado, sería muy valioso desarrollar un buen articulado en materia de medidas preventivas, especialmente las relacionadas con privacidad desde el diseño y por defecto y protección de datos por diseño y por defecto, así como las evaluaciones de impacto en materia de categorías especiales de datos personales. Estas dos herramientas podrían ser determinantes, junto con la definición y el reconocimiento como dato sensible en la ley mexicana, para reducir al mínimo los riesgos en torno al tratamiento de datos sensibles. Estas herramientas, muy especialmente la evaluación de impacto, permitiría hacer una valoración previa al tratamiento de cualquier dato sensible, sobre le necesidad y proporcionalidad del "uso" que se pretende llevar a cabo.

3.2.1 Efecto jurídico del reconocimiento específico de los datos biométricos y la cultura de privacidad y protección de datos

La definición y especificación de los datos sensibles en la LFPDPPP es buena en la medida que responde a los estándares internacionales en la materia, aunque es cierto que sí podría contener algunas especificaciones adicionales que ayudarían a fortalecerla, como es el hecho de, en primer lugar, incluir la mención de datos biométricos en su apartado del artículo 3° de la ley en comento y todo lo que eso conlleva, además de especificar ciertas categorías especiales de tratamiento, así como también establecer sanciones especiales en caso de tratamiento indebido de éste tipo de datos sensibles. El efecto jurídico de este reconocimiento sería importante, ya que por el simple hecho de especificar un hecho jurídico en la ley como lo es un dato biométrico (ya que el tenerlo no necesariamente implicó una voluntad de *tenerlo*) el acto jurídico donde se involucraron esos datos, ya sea voluntaria (como puede ser el consentimiento de los términos y condiciones por un servicio digital, un trabajo, etcétera, entre un usuario y un particular) o involuntariamente (como puede ser la tecnología de reconocimiento facial en áreas públicas, entre otras) éste acto jurídico sería reconocido, y por lo tanto debería estar acorde al respeto de los lineamientos que la ley establece, siendo este caso la ley de protección de datos,

donde quedaría especificado el tipo de consecuencias por el hecho de hacer o dejar hacer lo pertinente en el tratamiento de datos biométricos; por lo tanto el efecto jurídico inmediato sería que los particulares deberían contemplar dentro de su tratamiento el reconocer los datos biométricos como datos especialmente sensibles, con la distinción de que debieran merecer una categoría especial de tratamiento, ya que comprometen no solo la privacidad, sino la intimidad misma de las personas. Reforzaría la cultura de la seguridad de datos entre particulares. Un dato personal te hace identificable, pero un dato biométrico, en conjunto con otros datos sensibles y personales, te puede autentificar frente a terceros. El riesgo mayor tal vez no radica en aquellos sistemas donde previamente el usuario ya está registrado, porque ya dio su consentimiento (y que al mismo tiempo no dichos sistemas o *software* queda exento de ser manipulado por intereses diversos) sino sobre todo en la tecnología biométrica implementada en espacios públicos, como el reconocimiento facial, supuestamente por motivos de seguridad.

Como es bien sabido, los efectos jurídicos son aquellos hechos humanos, voluntarios y lícitos que tienen como fin inmediato la creación, extinción y modificación de un derecho. En el caso del reconocimiento de los datos biométricos los cuales en la mayoría de las legislaciones alrededor del mundo los identifican como datos especialmente protegidos a través de la creación de un derecho, el efecto jurídico de hacerlo sería reconocer explícitamente el derecho a la autodeterminación informativa del titular frente a los particulares que obtienen ganancias económicas inmensas derivado del tratamiento de datos personales, situación que se considera justificada en la medida que los datos biométricos son identificadores únicos de cada persona y que su utilidad social en el ámbito digital es muy elevada.

El efecto social, por otro lado, también es importante incentivarlo, al fomentar una cultura de la privacidad y protección de datos cada vez más creciente entre los usuarios de servicios digitales, ya que a pesar de la importancia del tema no muchos están familiarizados con el mismo, y esto provoca una brecha de seguridad iniciada por el mismo usuario que se inmiscuye en los servicios digitales que los particulares ofrecen sin conocer sus propios derechos.

Por otro lado, es de suma importancia que esa cultura de privacidad y protección de datos sea conocida sobre todo por los particulares, aquellas empresas

o corporaciones internacionales que ofrecen servicios digitales, o bienes a través de medios digitales por ejemplo. Ésta cultura de privacidad y protección de datos a particulares se puede traducir en algunos puntos que se resumen a continuación, tales como buenas prácticas, al reforzar las medidas de ciberseguridad con las últimas tecnologías que garanticen la mayor seguridad de los datos, adoptando tecnología *blockchain* por ejemplo; realizar evaluaciones de impacto en el tratamiento de datos biométricos como un medio de amortiguamiento del efecto de un indebido tratamiento; considerar políticas de transparencia en decisiones automatizadas o analítica; y garantizar la protección de datos biométricos por diseño y por defecto, entre otros.

A su vez sería prudente realizar en nuestro país una Carta de los Derechos Digitales tal como la tiene España, donde se reconozcan estos y otros derechos, tales como la identidad en el entorno digital, el derecho al pseudonimato, el derecho a no ser localizado y perfilado, el derecho a la seguridad digital, la herencia digital, la igualdad y la no discriminación en el entorno digital, la protección de menores, personas con discapacidad y personas mayores en el entorno digital, la neutralidad de Internet, la libertad de expresión e información, la participación ciudadana por medios digitales, la educación digital, etcétera. Los derechos digitales sin duda alguna coadyuvarían a proteger los datos biométricos de un mal tratamiento, ya que al actualizarse el funcionamiento del ecosistema digital, apertura áreas especializadas de tratamiento donde sin duda están siendo tratados datos personales y datos biométricos.

3.2.2 Las evaluaciones de impacto en el tratamiento de datos biométricos como medio de amortiguamiento

A decir del propio INAI a través de la Guía para la elaboración de evaluaciones de impacto a la privacidad[62], se puede advertir la importancia de las mismas, donde se menciona que “las evaluaciones de impacto en la protección de datos personales constituyen herramientas que permiten implementar un enfoque de privacidad por diseño, en concordancia con las mejores prácticas internacionales”[63]

[62] INAI, “Guía para la elaboración de evaluaciones de impacto a la privacidad” Ciudad de México, diciembre 2020 *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/guiaeip.pdf*
[63] Idem, p. 7

Por otro lado el artículo 35 del RGPD establece que ante la posibilidad de que un tratamiento implique un riesgo para los derechos y las libertades de las personas físicas, de forma proactiva la empresa deberá realizar una Evaluación de Impacto a la Protección de Datos, antes de poner en operación el tratamiento.

El tratamiento de los datos biométricos en la mayoría de los casos implica un gran riesgo de garantizar el derecho a la privacidad, intimidad y autodeterminación informativa, por lo que sería factible que los responsables del tratamiento de datos biométricos en posesión de los particulares incorporasen dentro de su actuación las Evaluaciones de Impacto de datos biométricos como buenas prácticas, previo a llevar a cabo un nuevo tratamiento de datos o una modificación sustancial a un tratamiento ya existente, así como la práctica de la Ética digital por diseño y por defecto que sostiene Manuela Battaglini Manrique de Lara[64].

3.2.3 Transparencia en los procesos de decisiones automatizadas

Los problemas éticos en los que incurren las empresas derivados de los procesos de decisiones automatizadas que toman para realizar algún trabajo de predicción de perfiles personales de acuerdo a la finalidad del negocio por ejemplo, siempre han estado en tela de juicio. Los parámetros que utiliza el área de recursos humanos de cierta empresa a través de algún *software* respectivo*,* en los cuales se establece la “idoneidad” o la “puntuación” que el algoritmo le da a alguna persona a través de cierta predicción (tal como *software* de contratación de personas o aseguradoras), nunca han sido trasparentes y siempre se escoltan detrás del secreto comercial o la propiedad intelectual.

Es por ello que la transparencia debe abarcar más allá de los datos de entrada que se almacenan en las bases de datos o archivos. Debe abarcar precisamente hasta el punto donde se toman las decisiones automatizadas y el *training set,* siendo el área donde choca con las directivas de secretos comerciales, derechos de propiedad intelectual y los *software* propietarios.

Como posible solución se propone el seguimiento de una política de privacidad robusta basada en las ideas de responsabilidad proactiva, transparencia, lealtad y

[64] Es una abogada y consultora, experta en privacidad, ética digital, marketing digital y comunicación *https://es.wikipedia.org/wiki/Manuela_Battaglini*

confidencialidad, así como la privacidad por diseño y por defecto, y sobre todo la Ética desde el diseño y por defecto que propone Manuela Battaglini[65], acompañado de buenas prácticas de protección de datos dentro del tratamiento, tal como la seudonimización, la anonimización y la disposición de *software open source.*

3.2.4 Privacidad por diseño y por defecto y Ética digital

Los procesos establecidos por los diseñadores que delimitan el funcionamiento y operatividad de un *software* "predictivo" que funciona a través de algoritmos en una tecnología, ya sean en un sistema, programa, plataforma, aplicación, etcétera, debe siempre tener en cuenta que a través del diseño y defecto de la misma todos ganen, especialmente el usuario, que a veces es visto como un simple conjunto de datos, pero realmente es su privacidad e intimidad como persona la que podría ser vulnerada. Es por eso que en los esquemas de negocio se debe considerar las políticas de privacidad necesarias donde impere la importancia de la protección y garantía de la información privada.

En ese sentido, la privacidad por diseño se entiende como una herramienta necesaria para asegurar y garantizar la protección de datos y la privacidad del usuario frente al interés de las corporaciones en su afán de recabar la mayor parte de información personal, sobre todo cuando no existe una cultura de protección de datos personales, cumplimiento normativo *compliance*, la responsabilidad activa y proactiva, así como la rendición de cuentas o *accountability*

El objetivo de la privacidad por diseño es dotar al sistema de medidas que protejan la información recabada del usuario durante todo el tiempo su interacción con el mismo, además de utilizar medios de minimización de datos, tal como la seudonimización, la anonimización y la disposición de *software open source.*

La jerga jurídica Europea en materia de protección de datos personales ha identificado siete principios que nutren la idea de privacidad por diseño y por defecto, a saber:

[65] La esencia es: no se permite la recolección de datos personales si el problema puede ser resuelto anónimamente. Ejemplo, protocolo DP-3T. En caso de que la Ética desde el diseño y por defecto no fuese aplicada, las posibilidades de evitar el daño y de arreglar los problemas éticos y de privacidad se reducen considerablemente. *https://centrodeestudios.ift.org.mx/admin/files/detevento/1627319079.pdf*

1. Diseño proactivo, no reactivo (Preventivo y no correctivo).
2. Privacidad como configuración por defecto.
3. Privacidad incrustada en el diseño.
4. Funcionalidad total: “Suma Positiva” no “Suma Cero”.
5. Seguridad en todo el ciclo de vida (*End to End*).
6. Visibilidad y Transparencia (*Keep it Open*).
7. Respeto a la Privacidad Personal (*User Centric*).

Cabe mencionar que en este ámbito de la privacidad por diseño y por defecto, dentro de las reglamentaciones comparadas, el único que la contempla expresamente en su contenido es el RGPD en su artículo 25, mientras que por otra parte, en la LFPDPPP, aunque no lo menciona expresamente, si alude al mismo en su artículo 14 cuando dice “En términos de los artículos 6 y 14 de la Ley, el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano. Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.” Dejando entrever que es necesario que las empresas o personas físicas tomen en cuenta la privacidad por diseño y por defecto ya que es una medida sumamente necesaria al momento de dar tratamiento de datos personales, y que decir al momento de hacerlo frente a datos de carácter sensible como lo son los datos biométricos, y que deberían ser datos particularmente protegidos expresamente reconocidos por las leyes.

La privacidad por diseño y por defecto, en conjunto con la ética desde el diseño y por defecto, deben concebirse como elementos esenciales y fundamentales para el buen funcionamiento y operatividad de la tecnología a desarrollar, debiendo abarcar en todos sus procesos, cuestiones que deberían darse de forma proactiva por la empresa y no esperarse a que la forma coercitiva de la ley lo imponga a las mismas.

3.3 Conclusiones preliminares del capítulo III

Los resultados de los once puntos contrastados de las leyes comparadas, proporciona elementos que en su momento podrían incluirse o reconocerse en la ley mexicana, y de esta forma expandir el espectro de protección de datos personales,

incluyendo por su supuesto los derechos digitales. Como ya se mencionó anteriormente, la definición de datos biométricos y su reconocimiento como dato especialmente sensible es de las más importantes, al igual que los tipos de categorización del tratamiento de datos personales, los procesos de tratamiento a gran escala, la extensión de los derechos de las personas, y las infracciones pormenorizadas del tratamiento de datos. Todas las consideraciones que resaltan de los puntos contrastados, ponen de manifiesto las actualizaciones que se puedan hacer en la LFPDPPP en torno al tema de los datos biométricos.

El efecto jurídico del reconocimiento de los datos biométricos con fines de autentificación sería el que los particulares deberían reconocer que la privacidad y la intimidad está en juego dentro del tratamiento de este tipo de datos, y por lo tanto, para hacer uso de los mismos, tengan bien delimitado en la ley la categoría especial de tratamiento, así como la sanción en que puedan incurrir por un mal tratamiento, ya sea en actos consensuados o por encontrarse en el área pública donde pueda ser objeto de grabación y análisis.

Por otro lado el efecto social de fomentar la cultura de la privacidad y protección de datos, ya sea entre usuarios como entre particulares, es de suma importancia para alcanzar un equilibrio entre el prestador de servicios y el usuario, cliente o trabajador, que al consensuar un acto jurídico, obtienen igualmente grado de responsabilidad tanto en el ejercicio como en el cumplimiento de éstos derechos y obligaciones, sin perder de vista que el usuario es en quien debería recaer la suplencia de la ley para proteger y garantizar sus derechos humanos: la privacidad y la intimidad.

La cultura de la privacidad y protección de datos que los negocios particulares deben considerar, debe estar siempre presente, tanto en aquellas empresas ya consolidadas como cualquier emprendedor que realice un negocio a partir de datos personales. Las buenas prácticas, reforzar medidas de ciberseguridad con tecnología *blockchain*, realizar evaluaciones de impacto en el tratamiento de datos biométricos, considerar políticas de transparencia en decisiones automatizadas y garantizar la protección de datos biométricos por diseño y por defecto, son unas de las que se puedan proponer.

El desarrollo de Internet y la sociedad digital ha cambiado radicalmente la forma en como interactuamos como sociedad, siempre existiendo el riesgo en materia de seguridad, privacidad y confianza en el mundo digital, por lo que, a decir del Dr. Julio Téllez[66] "El objetivo ahora es acometer la tarea de reconocer un espectro aún más amplio de derechos digitales de la ciudadanía. Así como garantizar que los derechos y libertades de los que se disfrutan en la vida offline están igualmente protegidos en el ámbito online"[67] Es de suma importancia que a la brevedad se distingan los derechos digitales para los mexicanos que naveguen en internet y aún fuera del mismo, tal como España y la U.E. son referentes.

[66] Doctorado en Informática Jurídica y Derecho de la Informática por el Instituto para la Investigación y Tratamiento de la Información Jurídica (I.R.E.T.I.J.), Montpellier, Francia 1981.
Investigador de tiempo completo en el área de Derecho y Nuevas Tecnologías en el Instituto de Investigaciones Jurídicas de la UNAM (IIJ-UNAM). Miembro del Sistema Nacional de Investigaciones (SNI-CONACYT). Multiconferencista nacional e internacional en temas de Derecho y Nuevas Tecnologías. *https://www.sitios.scjn.gob.mx/sitj-2016/node/36.html*

[67] Dr. Julio Alejandro Téllez Valdés "Los derechos digitales y la necesidad de su regulación" *INFO Ciudad de México*, diciembre, 2020. p.19 *https://infocdmx.org.mx/documentospdf/2021/Vinculacion/LosDerechosDigitales_Libro_impresion.pdf*

CONCLUSIONES

PRIMERA.- La autodeterminación informativa puede estar comprometida en el tratamiento de datos biométricos con fines de identificación y autentificación, por lo que es pertinente que estén debidamente regulados en las leyes de protección de datos, ya que de forma histórica y conceptual justifica su relación con los derechos humanos a la personalidad, específicamente a la vida privada.

SEGUNDA.- Al ser la información uno de los bienes más preciados en la actualidad, sobre todo desde la perspectiva de los entes económicos y financieros, es de suma importancia que se armonice legalmente su tratamiento cuando se trate de datos personales, para así evitar que toda recopilación de información no se traduzca en la invasión de la esfera más subjetiva de la persona, homogeneizando las leyes aplicables a entidades financieras con las de protección de datos, al igual que éstas queden supeditadas a la jurisdicción de las autoridades designadas constitucionalmente para ello.

TERCERA.- El contraste comparativo entre sistemas jurídicos diversos y similares de diversos países, logra robustecer la imperiosa necesidad de actualizar la ley mexicana de datos personales en posesión de particulares, ya que en dicha comparativa se extiende el espectro de protección de datos sensibles cada vez más urgente en la época digital.

CUARTA.- Se confirma parcialmente la hipótesis de que, si bien la ley mexicana de protección de datos en posesión de particulares no impide la protección de datos biométricos, ésta debe actualizarse conforme a los estándares internacionales, tales como ampliar el espectro de los derechos de las personas, delimitar categorías especiales de tratamiento, así como actualizar las sanciones pertinentes en el caso de un tratamiento indebido de datos biométricos, entre otros resultados previamente mencionados.

QUINTA.- Los resultados de la comparación entre leyes de protección de datos en torno a los datos biométricos entre la Unión Europea, España y México ofrecen una gama de referencias que en su momento se podrían incursionar en la jerga legal

mexicana, para así garantizar ampliamente el derecho a la autodeterminación informativa en la época digital, contemplando incluir los derechos digitales que sin duda garantizan de fondo una relación jurídica equilibrada en el entorno digital entre los particulares y los usuarios.

SEXTA.- Independientemente de lo regulado en la ley de protección de datos, es de suma importancia el que se fomenten y se practiquen buenas prácticas por parte de particulares en torno a la cultura de la privacidad y datos personales, donde la persona titular de los datos sea el centro y no la circunferencia. Tanto las evaluaciones de impacto, prácticas de transparencia en el procesamiento de datos y la privacidad por diseño y por defecto y la ética desde el diseño y por defecto, deben concebirse como elementos esenciales y fundamentales para el buen funcionamiento y operatividad de la tecnología a desarrollar

FUENTES DE INFORMACIÓN

BIBLIOGRÁFICAS

Álvarez, T. Y. (28 de agosto de 2019). Identidad en la era digital: Entre datos biométricos y pivacidad. Colima, Colima, México. Obtenido de https://recursos.ucol.mx/observatic/identidad-en-la-era-digital-entre-datos-biometricos-y-privacidad/

Becerril, S. A. (mayo-junio de 2010). Acuerdos Internacionales para la privacidad de la información. (M. e. Astorga, Ed.) Seguridad, cultura de preveción para Ti.(06), 3. Recuperado el 12 de octube de 2019, de https://revista.seguridad.unam.mx/sites/default/files/revistas/pdf/num_06_0.pdf

Cortés Osorio, j. a., Medina Aguirre, f. a., & Muriel. (diciembre de 2010). sistemas de seguridad basados en biometría. scientia et technica, XVII (46), 19, 20. Recuperado el 31 de 10 de 2019, de https://www.redalyc.org/pdf/849/84920977016.pdf

Cota, A. M. (2008). Consideraciones durante el proceso comparativo. Scielo . Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332008000100007

Díaz, M. (2018). El cuerpo como Dato. Obtenido de América latina: Derechos Digitales: https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf

Española, R. A. (s.f.). Diccionario de la Real Academia Española. Recuperado el 2020, de https://dle.rae.es/

Fernández, J. W. (2019). Derecho a la identidad. La cobertura del registro en México. Ciudad de México: Registro Nacional de Población. Obtenido de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2019/EstSociodemo/identidad2019.pdf

Gobierno de España. (6 de diciembre de 2018). Boletín Oficial del Estado. Obtenido de https://www.boe.es/eli/es/lo/2018/12/05/3

Gonzalez, A. G. (2005). El derecho a la intimidad desde una perspectiva constitucional: equilibrio, alcances, límites y mecanismos de protección,. México: Universidad Michoacana de San Nicolás de Hidalgo, Biblioteca de la Facultad de Derecho y Ciencias Sociales.

Gonzalez, P. C. (2001). Derecho de la comunicación en Internet. España: Colex. Editorial Constitucion y leyes.

Guía para el tratamiento de datos biométricos. (Marzo de 2018). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado el 21 de octubre de 2019, de Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales: http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf

Gutierrez, F. (15 de agosto de 2019). Identidad biométrica en CURP apoyará identificación digital en la banca: SHCP. El economista. Obtenido de https://www.eleconomista.com.mx/sectorfinanciero/Identidad-biometrica-en-CURP-apoyara-identificacion-digital-en-la-banca-SHCP-20190815-0130.html

Gutierrez, L. I. (2009). Alcances de una ética en el ciberespacio o el "giro" hacia una "ética floreciente". (P. U. Javeriana, Ed.) redalyc, 91-107. Recuperado el 26 de febrero de 2021, de https://www.redalyc.org/articulo.oa?id=86020246006

IFAI. (2014). Metodología de Análisis de Riesgo. MÉXICO. Obtenido de https://sontusdatos.org/wp-content/uploads/2013/04/ifai-metodologia-de-Riesgo-BAA_2014.pdf

INAI. (febrero de 2021). Obtenido de https://home.inai.org.mx/wp-content/uploads/TratamientoDP_FINTECH.pdf

INAI. (s.f.). Cinvestav. Obtenido de https://www.cinvestav.mx/Portals/0/sitedocs/tyr/GuiaTitulares-02_PDF.pdf

INAI. (s.f.). Guía para la elaboración de evaluaciones de impacto a la privacidad. Ciudad de México, México. Obtenido de https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/guiaeip.pdf

Introducción a la Ley General de Datos Personales en Posesión de Sujetos Obligados. (Diciembre de 2017). Instituto Nacional de la Economía Social. (INAI, Productor) Recuperado el 12 de octube de 2019, de Instituto Nacional de la Economía Social: http://www.inaes.gob.mx/doctos/pdf/transparencia/manual%20LGDPPSO.pdf

ITEI, I. d. (8 de Julio de 2021). Categorías, datos sensibles y datos biométricos y Uso de Datos Biométricos en el sector privado. Recuperado el 4 de marzo de 2021, de https://www.youtube.com/watch?v=xw-ppuZskF0&t=342s

Julián Felipe, M.-L. (marzo-junio de 2015). Gestión de la Indentidad Biométrica en las Organiaciones. 3C TIC, 4(1), 70-75. Obtenido de https://www.3ciencias.com/wp-content/uploads/2015/03/GESTI%C3%93N-DE-LA-IDENTIDAD-BIOM%C3%89TRICA-EN-LAS-ORGANIZACIONES.pdf

Martín, N. G. (2010). Sistemas jurídicos contemporáneos. México: Nostra ediciones.

Martín, N. G. (2010). Sistemas jurídicos contemporáneos. Ciudad de México, México: Nostra Ediciones. Recuperado el 12 de junio de 2021, de https://bibliotecavirtualceug.files.wordpress.com/2017/06/sistemas-juridicos-nuria-gonzalez.pdf

Pérez, G. S. (2012). Seguridad biométrica. Seguridad biométrica. Tepic, Nayarit: Universidad Autónoma de Nayarit. Obtenido de http://www.uan.edu.mx/es/comunicados/conferencia-magistral-seguridad-biometrica

Puente, C. (17 de marzo de 2021). La importancia de la técnica legislativa. Obtenido de Foro Jurídico: https://forojuridico.mx/la-importancia-de-la-tecnica-legislativa/

RAE. (s.f.). Diccionario de la Real Academia Española. Recuperado el 12 de agosto de 2020, de https://dle.rae.es

Rodríguez, V. D. (Enero-junio de 2013). Sistemas biométricos en materia criminal: un estudio comparado. Revista IUS, 7(31). Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100003

Tablado, F. (23 de marzo de 2020). Grupo Atico 34. Obtenido de https://protecciondatos-lopd.com/empresas/compliance/

Ucciferri, L. (20 de abril de 2017). la identidad que no podemos cambiar: cómo la biometría afecta nuestros derechos humano. Recuperado el 12 de octubre de 2020, de https://adc.org.ar/informes/la-identidad-que-no-podemos-cambiar-biometria-sibios/

Ucciferri, L. (2017). la identidad que no podemos cambiar: cómo la biometría afecta nuestros derechos humanos. Obtenido de Asociación por los Derechos Civiles de Argentina: https://adc.org.ar/informes/la-identidad-que-no-podemos-cambiar-biometria-sibios/

Unidos, D. d. (2017). El libro de referencia de las huellas dactilares. Washinton DC. Obtenido de https://www.ncjrs.gov/pdffiles1/nij/249575.pdf

Valdés, J. A. (Diciembre de 2020). Los derechos digitales y la necesidad de su regulación. Ciudad de México, México.

Fuentes jurídicas

Unión Europea, E. P. (2016). Reglamento General de Protección de Datos. Unión Europea: Diario Oficial de la Unión Europea.

BOE, J. d. (2018). ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (3/2018). España.

Consejo de Europa. (28 de enero de 1981). Boletín Oficial del Estado, Gobierno de España. Recuperado el 12 de octubre de 2019, de Boletín Oficial del Estado, Gobierno de España: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

Consejo de Europa. (28 de septiembre de 2001). Diario Oficial de la Federación, Secretaría de Gobernación. Recuperado el 12 de octubre de 2019, de Diario Oficial de la Federación, Secretaría de Gobernación: https://dof.gob.mx/nota_detalle.php?codigo=5539474&fecha=28/09/2018

Ley Federal de Protección de Datos Personales en Poseción de los Particulares. (5 de julio de 2010). Camara de Diputado del H. Congreso de la Union. Recuperado el 12 de octube de 2019, de Camara de Diputado del H. Congreso de la Union: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (21 de diciembre de 2011). Camara de Diputados del H. Congreso

de la Unión. Recuperado el 21 de octubre de 2019, de Camara de Diputados del H. Congreso de la Unión: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

OTROS:

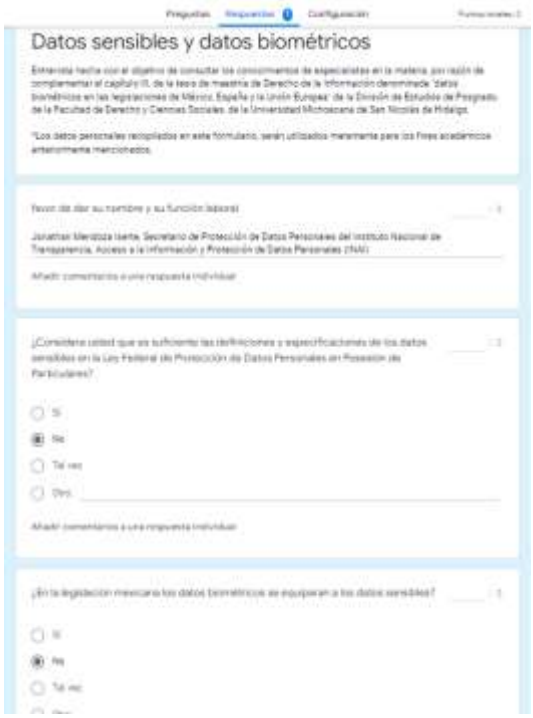
La información vertida se obtuvo de una entrevista realizada a Jonathan Mendoza Iserte, Secretario de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), quien a través de redes sociales, se le consultó la posibilidad de entrevistarlo a través de un formulario, para tener conocimiento del reconocimiento de datos biométricos en la ley mexicana, el cual se le envió vía correo electrónico el día 9 de noviembre del 2021 y tuvo la amabilidad de responderlo y devolverlo el día 11 de noviembre del 2021

ANEXOS

ENTREVISTA REALIZADA A JONATHAN MENDOZA ISERTE, SECRETARIO DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI)

La información vertida se obtuvo de una entrevista realizada a Jonathan Mendoza Iserte, Secretario de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), quien a través de redes sociales, se le consultó la posibilidad de entrevistarlo a través de un formulario para tener conocimiento del reconocimiento de datos biométricos en la ley mexicana, el cual se le envió al correo electrónico jonathan.mendoza@inai.org.mx el día 9 de noviembre del 2021 y tuvo la amabilidad de responderlo y devolverlo el día 11 de noviembre del 2021.

La entrevista constó de diez preguntas de temas relacionados con los datos biométricos y su forma de regulación en las legislaciones de la Unión Europea, España y México.



Preguntas Respuestas 9 Configuración

Datos sensibles y datos biométricos

Entrevista hecha con el objetivo de consultar los conocimientos de especialistas en la materia, por razón de complementar el capítulo III, de la tesis de maestría de Derecho de la Información denominada "datos biométricos en las legislaciones de México, España y la Unión Europea" de la División de Estudios de Posgrado de la Facultad de Derecho y Ciencias Sociales de la Universidad Michoacana de San Nicolás de Hidalgo.

"Los datos personales recopilados en este formulario, serán utilizados únicamente para los fines académicos anteriormente mencionados.

Favor de dar su nombre y su función laboral

Jonathan Mendoza Iserte, Secretario de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

Añadir comentarios a una respuesta individual

¿Considera usted que es suficiente las definiciones y especificaciones de los datos sensibles en la Ley Federal de Protección de Datos Personales en Posesión de Particulares?

- Sí
- **No**
- Tal vez
- Otro:

Añadir comentarios a una respuesta individual

¿En la legislación mexicana los datos biométricos se equiparan a los datos sensibles?

- Sí
- **No**
- Tal vez

¿Cree usted que haría falta incluir alguna definición y especificación de los datos biométricos en la Ley Federal de Protección de Datos Personales en Posesión de Particulares?

- **Sí**
- No
- Tal vez
- Otro:

Añadir comentarios a una respuesta individual

En el Reglamento General de Protección de Datos de la Unión Europea se especifican tres tipos de categorización del tratamiento de datos personales, siendo categorías especiales los relacionados a los datos genéticos, datos biométricos y datos de salud. ¿Cree usted que debería reconocerse en la LFPDPPP este tipo de categorización de tratamiento para reforzar la protección de la privacidad en México?

- Sí
- No
- **Tal vez**
- Otro:

Añadir comentarios a una respuesta individual

¿Qué opinión le merece el caso de la excepción de las Entidades Financieras de los sujetos regulados de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en relación a los datos biométricos? ¿Deberían incluirse dentro de lo regulado por esta ley o se deberían especificar regulaciones por la Comisión Nacional Bancaria y de Valores?

Deberían incluirse dentro de la regulación de protección de datos personales en posesión de los particulares, ya que no emerita ningún supuesto de excepción.

A pesar que ni siquiera se mencionan los datos biométricos en la legislación mexicana en comento, pero que se interpreta que estos pertenecen a los datos sensibles ¿Considera usted que existen los medios legales para garantizar su protección frente al tratamiento de datos de operadores extranjeros?

- Sí
- No
- Tal vez
- **Otro:**

Se abordan dos temas distintos en esta pregunta, que no necesariamente conllevan una correlación. Por un lado, la protección de datos personales sensibles y, por el otro, la jurisdicción y competencia de la autoridad garante. Asimismo, menciona operadores extranjeros sin distinguir en qué supuesto de la Ley se encuentran dichos operadores. Finalmente, es importante mencionar que el artículo 4 del Reglamento de la LFPDPPP que pudiera dar respuesta al cuestionamiento de forma integra.

Añadir comentarios a una respuesta individual

Dentro del procesamiento de información del sistema biométrico existen varios subsistemas en donde existe el riesgo latente de un tratamiento ilegal de los datos personales con fines diversos ¿Cree usted que se debería regular legalmente su procesamiento- tratamiento desde la recolección de datos hasta el almacenamiento de los mismos?

- Sí
- No
- Tal vez
- **Otro:**

Se encuentra regulado en el capítulo II del Reglamento de la LFPDPPP y en los artículos 19, 20 y 21 de la LFPDPPP.

Añadir comentarios a una respuesta individual

Para lograr lo anterior, ¿Considera usted que sería menester incluir dentro de la Ley Federal de Protección de Datos Personales en Posesión de Particulares un capítulo específico en relación a las infracciones y sanciones específicas de las categorías especiales?

- Sí
- No
- Tal vez
- **Otro:**

Existen dos capítulos específicos sobre el procedimiento de imposición de sanciones y de infracciones (capítulos IX y X).

Añadir comentarios a una respuesta individual

La transferencia de datos personales a terceros es una situación delicada y cada vez más común en la globalización digital, debido a que se considera una violación a los derechos del titular cuando se realiza cierto tratamiento sin el consentimiento del interesado por empresas ¿La protección de datos biométricos está reconocida en la legislación mexicana frente a estos hechos?

- **Sí**
- No
- Tal vez
- Otro:

Añadir comentarios a una respuesta individual

¿Le gustaría incluir algún comentario en general que le provoque expresar en torno a los datos biométricos y la necesidad mexicana de su regulación y especificación? ¿O considera que es suficiente lo establecido en la Ley Federal de Protección de Datos Personales en relación a los datos sensibles?

Sería importante conceptualizar el término y cuándo dichos tratamientos pertenecen a categorías especiales de datos personales.