Datos Personales Biométricos

¿Qué son y cómo protegerlos?

Dra. María de los Ángeles Guzmán García

Impreso en México
1ª edición: diciembre 2021

Autora:
MARÍA DE LOS ANGELES GUZMÁN GARCÍA

Diseño de cubierta: Ernesto González Tapia
Diseño y formación: Jorge Romero Ortega

Registro en trámite

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO
2021

PLENO DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO

Julio César Bonilla Gutiérrez
Comisionado Presidente del INFO CDMX

Laura Lizette Enríquez Rodríguez
Comisionada Ciudadana del INFO CDMX

Arístides Rodrigo Guerrero García
Comisionado Ciudadano del INFO CDMX

María del Carmen Nava Polina
Comisionada Ciudadana del INFO CDMX

Marina Alicia San Martín Rebolloso
Comisionada Ciudadana del INFO CDMX

Libro divulgativo:

Datos personales biométricos
¿Qué son y cómo protegerlos?

María de los Angeles Guzmán García[1]

1 Doctora en Estudios Superiores de Derecho Constitucional por la Universidad Complutense de Madrid. Máster en Diplomacia y Relaciones Internacionales por la Escuela Diplomática de Madrid. Maestra en Derecho Constitucional y Licenciada en Derecho por la Universidad Autónoma de Nuevo León. Profesora de la Universidad Autonóma de Nuevo León y Comisionada de la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León (angelesguzman@gmail.com).

Índice

Glosario 11
Introducción 13

I. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES 17
1. Generalidades de la Protección de Datos Personales. 17
2. Definición de datos personales 20
3. Derecho autónomo o derecho derivado 22
4. Bien jurídico protegido 25
5. Datos sensibles 26
5.1 Datos de salud 27
5.2 Datos genéticos 28
5.3 Datos biométricos 35

II. LOS DATOS BIOMÉTRICOS 36
1. Biometría 36
2. Datos biométricos 37
3. Algunas menciones en la legislación mexicana 41
4. Normativas locales de protección de datos personales 45
5. PANAUT 2021. 46
5.1 Objetivo 46
5.2 Contenido 47
5.3 Análisis 49

III. PROTECCIÓN DE LOS DATOS BIOMÉTRICOS 51
1. Riesgos y medidas de prevención 51
2. Derechos ARCO 53
2.1 Constitución Política de los Estados Unidos Mexicanos 56
2.2 Ley Federal de Protección de Datos Personales en Posesión de Particulares 56
2.3 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados 58
Conclusión 60
Bibliografía 62
Monografías y artículos científicos 62
Normativa mexicana 63
Normativa internacional 63
Sentencias 64

Glosario

ADN	Ácido desoxirribonucleico
ARN	Ácido ribonucleico
Art./arts.	Artículo/artículos
CDFUE	Carta de Derechos Fundamentales de la Unión Europea
CE	Consejo de Europa
DIDGH	Declaración Internacional sobre los Datos Genéticos Humanos
DUGH	Declaración Universal sobre el Genoma Humano
FIEL	Firma Electrónica Avanzada
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
INE	Instituto Nacional Electoral
InfoCDMX	Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de Particulares

LFTR	Ley Federal de Telecomunicaciones y Radiodifusión
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
LPDPPSOCDMX	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México
OCDE	Organización para la Cooperación y el Desarrollo Económico
PANAUT	Padrón Nacional de Usuarios de Telefonía Móvil
RGPD	Reglamento General de Protección de Datos Personales
SAT	Sistema de Administración Tributaria
STC	Sentencia del Tribunal Constitucional de España
TIC	Tecnologías de la Información y la Comunicación
UE	Unión Europea
UNAM	Universidad Nacional Autónoma de México

Introducción

La preocupación por ¿Qué son los datos personales biométricos? y ¿Cómo poder protegerlos? ha crecido en los últimos años debido a la aparición de múltiples sistemas de tecnología digital utilizados para reconocimiento, identificación y autenticación de las personas. Su estudio en México aún es reciente y apenas se puede observar en escasas legislaciones, alguna mención aislada al respecto, pero sin profundizar o definirlos adecuadamente.

A partir del incremento de la virtualización de la vida cotidiana, provocada por la pandemia del virus SARS-CoV-2, las personas se han dado cuenta de la vulnerabilidad de sus datos personales. De manera particular, han mostrado especial interés en saber qué son y cuáles serían las consecuencias que les implicaría la posible vulneración de sus datos biométricos, y cómo protegerlos.

El dato biométrico más utilizado para identificar a una persona lo representa la huella dactilar, desde hace varias décadas se usa de forma habitual, por ejemplo, para registros de asistencia en colegios, trabajos, gimnasios, etcétera. Y con la implementación de la inteligencia artificial en los teléfonos celulares su uso se ha potencializado, pues no solo se utiliza la huella dactilar para desbloquear las pantallas, sino que además se puede hacer a través del reconocimiento facial o del iris.

Las aplicaciones móviles, al igual que los centros de trabajo, también recaban datos personales y, en muchas ocasiones, los de índole biométrico para el reconocimiento, identificación o autenticación de quienes las utilizan. Incluso, existen aquellas dedicadas al ocio en donde con solo adjuntar una fotografía de quien sea se puede ver el envejecimiento, rejuvenecimiento y movimientos de la persona a través de la fotografía, hasta se les puede percibir interpretar una canción. La cuestión es que el rostro constituye un dato biométrico que las personas no protegen al uti-

lizar estas aplicaciones, lo que se agrava al adjuntar una fotografía ajena sin el consentimiento del titular.

En el ámbito público y privado también se usan o tratan los datos biométricos. Por ejemplo, las instituciones de gobierno, financieras y bancarias utilizan las huellas dactilares o la voz. En el ámbito público, el Instituto Nacional Electoral (en adelante INE), ha recabado siempre la huella dactilar para identificar a quienes integran el padrón electoral. Por su parte, los bancos usan un método de autenticación de la identidad personal el cual cruzan con la base de datos del INE, esto resulta cuando menos extraño, pues la finalidad con la que se le otorgan los datos personales a dicho instituto es la identificación de la persona para ejercer el derecho al voto. Por igual, el Sistema de Administración Tributaria (en adelante SAT) representa también un caso interesante, ya que, es requisito escanear el iris al momento de tramitar la firma electrónica (en adelante FIEL).

Datos personales biométricos ¿Qué son y cómo protegerlos?

Para situarse en el tema hace falta recordar qué son los datos personales y sus categorías especiales, como los datos sensibles. Por ello, es necesario precisar las definiciones de ambos conceptos, tal como se establecen en la legislación mexicana nacional, con independencia de que durante esta investigación se hace referencia de manera constante a instrumentos jurídicos europeos. Esto, debido a que la principal referencia en México se tiene en Europa, lugar donde tiene su origen el derecho a la protección de los datos personales.

Los "datos personales" consisten en cualquier información concerniente a una persona física identificada o identificable, y se considera de esta manera cuando su identidad pueda ser determinada directa o indirectamente a través de cualquier información (art. 2.IX LGPDPPSO). Particularmente, la ley de la materia de la Ciudad de México refiere que dicha información puede ser el nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona (art. 3.IX LGPDPPSOCDMX).

Por su parte, los "datos personales sensibles" son aquellos que se refieren a la esfera más íntima de la persona, o cuya utilización indebida pueda ocasionar discriminación o riesgo grave. La ley establece que, de manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual (art. 2.X LGPDPPSO). De manera adicional, a estos datos, la ley de la materia de la Ciudad de México establece los "datos biométricos" en la categoría de sensibles (art. 3.X LGPDPPSOCDMX).

Si bien en la definición de datos personales sensibles de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante LGPDPPSO), no aparecen los biométricos, lo cierto es que la opinión generalizada indica que sí pertenecen a dicha categoría, aunque no se describan de forma enunciativa, tal como sucede en el caso de la Ciudad de México.[2]

Ahora bien, los "datos personales biométricos" reflejan la biometría de cada persona, es decir, las medidas biológicas o físicas que la hacen única respecto a las demás. Estos pueden ser las huellas dactilares, ADN, geometría de la mano, características de iris y retina, forma de caminar y demás análogos (art. 62.IX Lineamientos LGPDPPSOCDMX).

2 La Comisión de Transparencia y Anticorrupción de la Cámara de Diputados aprobó el 23 de febrero de 2021 un dictamen para reformar la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. El texto final aprobado refiere que se incluirá en la categoría de datos sensibles la "información genética o biométrica dirigida a identificar de manera unívoca a una persona física", disponible en <http://gaceta.diputados.gob.mx/PDF/64/2021/feb/20210203-VI.pdf> (Consulta: 05/09/2021).

I. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

A partir del desarrollo de las nuevas tecnologías, los datos personales contenidos en ficheros o bases de datos, principalmente electrónicos, resultan cada vez más vulnerables a la apropiación y abuso por parte de quienes se encargan de su tratamiento.3 Lo cual intensifica la posibilidad de que cualquier persona pierda su anonimato. Por ello, se protege la puesta en común de datos aparentemente inocuos, frente a ilimitados almacenamientos, tratamientos y transferencias que se refieran a un individuo o que puedan ser individualizados (González Pascual, 2009: 948).

1.- Generalidades de la Protección de Datos Personales

El derecho humano a la protección de datos personales no es un derecho fundamental nuevo. Este se configura a partir de las concepciones que se tienen de la vida privada o intimidad, del derecho al honor y a la propia imagen.[4] La evolución de estos, principalmente el de la vida privada o privacidad, plantearon nuevas situaciones que fueron motivo de la creación de uno nuevo, la protección de datos personales.

El estudio de este derecho se sitúa en el campo de aquellos fundamentales, razón por la que resulta importante comprender su nueva inclusión dentro del catálogo de los mismos, tal como un derecho nuevo, ya sea

3 Por tratamiento se entiende cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales (art. 3.XXXIII LGPDPPSO).

4 El derecho al honor y a la propia imagen, como la protección de datos personales, constituyen derechos independientes entre sí, sin embargo, y como ocurre con otros, se relacionan entre sí (principio constitucional de interdependencia de los derechos humanos), principalmente con el derecho a la vida privada. Desde una perspectiva se podría decir que el derecho a la privacidad es el género, mientras que los otros son la especie, cada uno en su propio ámbito de aplicación. Ya que la vulneración de alguno afecta directamente la vida privada de la persona. Cabe recordar que el derecho a la protección de datos personales comprende el control por parte de la persona de su información personal, que puede o no, ser privada.

el de la protección de datos personales o bien el de autodeterminación informativa (Conde Ortiz, 2005: 27).

Hoy en día las vulneraciones a la intimidad por la obtención de perfiles personales se presentan cada vez de forma más grave. El Tribunal Constitucional alemán, en su Sentencia de 1983 contra la Ley del censo, establecía que, en virtud de la evolución de los condicionamientos tecnológicos, a través de los "perfiles personales" era posible producir una imagen total y pormenorizada de una persona, incluso en el ámbito de su intimidad. Esto convertía a su propio ciudadano en el llamado "hombre de cristal" (así citado por el propio Tribunal),[5] término que significaba la pérdida del anonimato porque el individuo se convertía en una persona conocida y, por lo tanto, frágil en el aspecto más profundo de su vida, es decir, su intimidad.

Por ello, no resulta extraña la notoria necesidad de proteger los "perfiles personales",[6] entendidos como los datos personales contenidos en los ficheros o registros almacendos en grandes bases de datos, información que puede dar un retrato fiel de la persona, especialmente para analizar o predecir su comportamiento. Fioriglio refiere que la *profilazione* (2008: 78-86), representa uno de los grandes desafíos de Internet, y lo define en general como la clasificación del comportamiento, el rastro de gustos, ideología, intereses, etcétera, que se deja en la red, y recuerda aquella frase sobre que cada uno es seguido por su pasado. Incluso, las *cookies* que se almacenan en los dispositivos portátiles contribuyen a la *profilazione.*[7]

Para el estudio de la protección de datos personales, Campuzano Tome (2000: 55) refiere que el tema de la salvaguarda de la vida privada y de los datos personales puede ser analizado desde una doble vertiente: la

5 Sentencia del Tribunal Constitucional alemán, de fecha 15 de diciembre de 1983, en contra de la Ley del Censo. *Boletín de Jurisprudencia Constitucional*, No. 33, 1984. p. 137-138.

6 El artículo 4 del Reglamento General de Protección de Datos Personales del Consejo de Europa, establece que por la elaboración de perfiles se entiende toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

7 Estas son pequeños fragmentos de texto que se envían al buscador y se almacenan en las computadoras, luego de visitar sitios web. Es decir, permiten que el navegador o buscador recuerde información sobre las visitas, haciendo más fácil volver a visitar los sitios para que resulten más útiles.

primera, que corresponde a la protección de dichos datos como objeto de valor en un sistema de mercado dirigido a instaurar el comercio electrónico como principal sistema de intercambio de bienes. Para tal caso, se habla de protección: a los consumidores, a los datos relativos al consumo, al comercio electrónico, de seguridad de las transacciones electrónicas, de nuevas formas de contratación. La segunda se refiere a la protección de los datos como medio de resguardo de la persona dirigido a salvaguardar uno de los principales derechos fundamentales, es decir, el de la vida privada.

Así, por un lado, el debate se centra sobre la protección de los consumidores y de los contratantes frente a las nuevas formas de difusión y divulgación de los datos emitidos a través de las redes digitales y, por otro, se habla de la protección de las personas frente a la "sociedad de la información".[8] Ambos modelos no son incompatibles, si bien parece lógico que, dado el carácter fundamental del derecho a la vida privada, se examinen con prioridad los instrumentos necesarios para otorgar a la ciudadanía, como persona –antes que como consumidor o contratante–, la adecuada protección ante las nuevas tecnologías. Ello sin perder de vista que tal garantía no se agota únicamente en los datos personales ya que, en la actual sociedad de la información, la noción de salvaguarda de la vida privada reviste un importante abanico de sectores. Para algunos, se trata del derecho a gozar de comunicaciones privadas, para otros, de no ser objeto de vigilancia o de hacer que sea respetado su cuerpo impidiendo la realización de determinadas prácticas. En definitiva, la protección de la vida privada debe ser explorada desde el ángulo de los derechos de la persona (Campuzano Tome, 2000: 55).

8 En este caso, se hace referencia a la sociedad de la información, en lo que hace a la tendencia digital (internet, telecomunicaciones, etc.), con sus ventajas y riesgos. Cabe señalar, que este término es interpretado de diversas formas como sociedad: del conocimiento, digital, de la comunicación, de la red, del ciberespacio, de telecomunicaciones, etcétera. (Ruiz de Querol y Buira, 2007: 18-21). La idea de la sociedad de la información tiene sus principales orígenes a partir de la década de 1970, a raíz de la revelación del proyecto, elaborado en 1973 por el Ministerio del Interior en Francia, de un sistema automatizado de ficheros administrativos y del repertorio de individuos (Safari), basado en la interconexión de cuatrocientos ficheros distintos mediante un "identificador único", el número de afiliación a la Seguridad Social. El gobierno federal de Estados Unidos presta atención al asunto de las telecomunicaciones y pone en circulación la expresión de "sociedad de la información" (en 1970, el presidente Richard Nixon cambia completamente el organigrama gubernamental de toma de decisiones en el ámbito de las tecnologías del cable, la informática y el satélite) (Mattelart, 2001: 118-121).

2.- Definición de datos personales

El derecho fundamental a la Protección de Datos Personales es definido por la Sentencia 290/2000 del Tribunal Constitucional de España como aquel que garantiza a la persona un poder de control y disposición sobre sus datos personales. Dicho derecho confiere a su titular un haz de facultades que conforman elementos esenciales del conjunto de principios y normas, integrado por la facultad que corresponde al afectado de consentir la recolección y el uso de su información individual y personal, así como a conocer las mismas. Para hacer efectivo ese contenido, incluye también, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo, a quien corresponda, que ponga fin a tener y emplear tales datos.[9]

En otras palabras, este nuevo derecho fundamental comprende un conjunto de principios y normas que la persona puede ejercer frente a quienes sean poseedores de ficheros públicos o privados; de saber el contenido, uso y destino de la información que se contenga en ellos. De suerte que en éstos han de proyectarse, en última instancia, las medidas destinadas a la salvaguarda de dicho derecho por parte de las administraciones públicas competentes.[10]

Para una correcta protección de datos personales, se considera fundamental hacer referencia a la definición que algunos ordenamientos hacen del concepto de "datos personales", y la finalidad que persigue cada uno de estos instrumentos:

A) Convenio No. 108 del Consejo de Europa de 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (arts. 1 y 2). Señala que

9 STC 290/2000 de 30 de noviembre, Fundamento Jurídico 7.
10 Ídem.

los *datos de carácter personal* son cualquier información relativa a una persona física identificada o identificable. Su finalidad es garantizar en el territorio de cada parte, a cualquier persona física sea cual fuere su nacionalidad o 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 (protección de datos).

B) Carta de los Derechos Fundamentales de la Unión Europea (en adelante CDFUE) de 7 de diciembre de 2000, señala que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones (art. 7 CDFUE). Asimismo, refiere que: 1) Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan; 2) Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de quien resulte afectado o en virtud de otro fundamento legítimo previsto por la ley. Cada individuo tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación; y 3) El respeto de estas normas quedará sujeto al control de una autoridad independiente (art. 8 CDFUE). La Carta tiene como objetivo compilar todos los derechos civiles, políticos, económicos y sociales de las personas ciudadanas en Europa, mismos que tienen relación con la dignidad, libertad, igualdad, solidaridad, ciudadanía y justicia.

c) El Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo (arts. 1 y 4). Refiere que los datos personales son toda información sobre una persona física identificada o identificable. Se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo el nombre, número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o

social.[11] El Reglamento tiene como finalidad proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.[12]

D) Ley Federal de Protección de Datos Personales en Posesión de los Particulares (arts. 1 y 3) de 27 de abril de 2010 (México).[13] Refiere que los datos personales son cualquier información concerniente a una persona física identificada o identificable. Esta 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.

E) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (arts. 1 y 3) de 13 de diciembre de 2016 (México).[14] Señala que los datos personales son cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. La Ley tiene entre sus objetivos el de garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales.

3.- Derecho autónomo o derecho derivado

Es importante contextualizar el derecho a la protección de datos personales como uno autónomo e independiente. En ocasiones, puede causar

11 Articulo 4.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

12 Articulo 2, inciso 1, del Reglamento general de protección de datos (UE) 2016/679.

13 Publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010.

14 Publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017.

alguna confusión con el de la privacidad o intimidad, ya que comparten rasgos particulares, como la protección a la vida privada de injerencias de terceros, por el uso indebido de la información personal, por ejemplo. Una diferencia entre ambos es que el derecho a la privacidad protege la vida privada en su ámbito más íntimo, como son las relaciones familiares; mientras que el de la protección de datos personales protege la información personal, ya sea privada o no, otorgando la facultad de controlar el uso, destino y permanencia de la misma en un fichero, por ejemplo, los datos profesionales en los registros de una asociación.

El derecho a la protección de datos personales, por su denominación, daría la impresión de que solo protege a los "datos", pero no es así, ya que protege a la persona de intromisiones ilegítimas en su vida privada, originadas por el uso de los datos personales. La inclusión de este nuevo derecho resulta trascendente, debido a que los datos aparentemente inocuos y acumulados con otros igualmente inofensivos, podrían arrojar un perfil personal,[15] y fácilmente se podría identificar a un individuo. De esta manera, las personas se vuelven altamente vulnerables ante la cantidad de información que las bases de datos almacenan.

Actualmente, la doctrina jurisprudencial del Tribunal Constitucional español (STC 292/2000) ha aclarado y agotado la posición de que el derecho a la autodeterminación informativa (protección de datos personales) forme o no parte del que corresponde a la intimidad personal o familiar. Si bien aquel surge a partir del derecho a la privacidad, su evolución ha sido tal que, hoy en día, tiene una mayor amplitud, la cual no le permite seguir en un ámbito tan delimitado como el derecho a la intimidad.[16]

15 Con relación a los perfiles personales Garriga Domínguez (2004: 25) dice que los datos pueden utilizarse de forma más o menos aislada, o bien, reunirse y confrontarse. Esta interrelación de las informaciones personales permitirá la obtención del perfil de cualquiera y servirá para que se adopten decisiones que le afecten sin que las personas *sean tenidas en cuenta ni consultadas*. El perfil, ya sea del consumidor, del internauta, del asegurado, del empleado, del estudiante o del profesor, económico, ideológico o sexual, permite obtener una *radiografía* de toda o de parte de su vida, así como prever –o al menos intuir– sus reacción y comportamientos futuros. El tratamiento de los datos personales *hace posible una vigilancia de hecho de la vida cotidiana del individuo*, al permitir el registro de una serie de datos que separadamente carecen de importancia, pero que adecuadamente relacionados permiten obtener el perfil de una persona.

16 Se aclara al lector que durante este trabajo se usa indistintamente la palabra privacidad e intimidad. Esto

El derecho a la protección de datos personales (autodeterminación informativa) y el de privacidad o intimidad representan derechos fundamentales directamente ligados a la dignidad humana, que comparten el *objetivo* de ofrecer una eficaz protección constitucional de la vida privada o familiar.

El *derecho a la privacidad* se caracteriza por un eminente "contenido negativo", pues salvaguarda del conocimiento ajeno una parte de la vida, aquella que se desea tener en el lado más reservado o secreto, como son las relaciones familiares. Además, coincide con los datos sensibles, entre otros: el origen étnico o racial, la tendencia sexual o política, el estado de salud, opiniones filosóficas. Este derecho otorga "obligaciones de no hacer", esto sucede cuando la persona que conoce algo de otra, está obligada a no dar a conocer lo así conocido. Su *función* es la de excluír del conocimiento ajeno algo.

Por su parte, el *derecho a la protección de datos personales*, otorga "obligaciones de hacer", pues el responsable del tratamiento está obligado a realizar una serie de acciones para garantizar el derecho humano y la seguridad de la información del titular, entre ellas, mostrar el aviso de privacidad. Asimismo, cumplir con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. Este derecho asegura a la persona un poder de control sobre sus datos personales, su uso y destino.

El derecho a la *protección de datos personales* o autodeterminación informativa, tiene un "objeto más amplio", pues la información de la persona puede o no ser privada, por ejemplo: el nombre, correo electrónico, número telefónico, información académica o laboral, es decir, aquella que no necesariamente arroja un perfil de la personalidad. Mientras que

debido a que el diferenciar ambos términos implicaría un estudio, análisis y discusión mayor, que sobrepasaría la finalidad de esta obra. En México se usa el término de derecho a la privacidad, mientras que España el de derecho a la intimidad. Muchas veces depende de dónde deriva la traducción de la influencia extranjera, si de la palabra *privacy* o *intimacy*. Además, *el derecho a la privacidad o intimidad* es distinto al *derecho a la protección de datos personales,* aunque este en su origen haya surgido a partir del primero. Dicho lo anterior, el presente estudio se enfoca en los datos biométricos en relación con el derecho a la protección de los datos personales.

la *privacidad* posee un "objeto más restringido", ya que la información se relaciona con la esfera más íntima, en particular: los vínculos familiares o los datos sensibles.

En este sentido, el tratamiento de la información personal podría o no, afectar información íntima o secreta que constituya el objeto de protección del derecho a la intimidad. De la misma forma, los datos personales informatizados no tienen necesariamente que arrojar un retrato personal que implique una valoración peyorativa u ofensiva de un individuo y que atente contra su buen nombre o fama (Garriga Domínguez, 2004: 22).

4.- Bien jurídico protegido

El derecho a la intimidad o privacidad por lo regular conlleva el poder jurídico de rechazar intromisiones ilegítimas en la esfera protegida y, de manera correlativa, decidir de forma libre y dentro de ella la propia conducta, se está pues frente a un típico derecho de defensa. Sin embargo, la técnica del derecho a la protección de datos personales resulta más compleja y amplia, ya que, por un lado, combina poderes del individuo frente a terceros (límites y prohibiciones) con diversas garantías instrumentales y; por otro, los datos que se protegen no tienen por qué ser íntimos, basta con que sean personales, aun cuando parezcan inofensivos (Ruiz Miguel, 2004: 241).

Por su parte, Ricard Martínez Martínez (2004: 47) señala que la información personal susceptible de revelar aspectos privados del individuo habrá de protegerse, ya sea por sí sola, o mediante su consideración conjunta con otra información o gracias a la realización de algún tipo de tratamiento.

Sin embargo, es importante aclarar que el derecho a la protección de datos personales no protege los datos *per se*, sino al titular de los mismos, porque la información por sí sola no implica un peligro, tan solo la asociación de esta con una determinada persona.

5.- Datos sensibles

Son aquellos que se refieren a la esfera más íntima de su titular, cuya utilización indebida pueda dar origen a *discriminación* o conlleve un riesgo grave para este. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.[17]

La Comisión de Transparencia y Anticorrupción de la Cámara de Diputados de México aprobó el 3 de febrero de 2021 un dictamen para reformar la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; cuyo texto final aprobado expresa que son datos personales sensibles:

> Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa más no limitativa, se consideran sensibles aquellos datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, creencias o *convicciones* religiosas, filosóficas o morales, *afiliación sindical*, opiniones políticas, *información relativa a la* preferencia u *orientación* sexual**,** información genética o *biométrica dirigida a identificar de manera unívoca a una persona física* (cursivas propias).

La normativa aplicable para la Ciudad de México señala que son datos especialmente protegidos (sensibles) el origen étnico o racial, las características morales o emocionales, la ideología, así como las opiniones

17 Artículo 3.X de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual (Art. 62.X Lineamientos LGPDPPSOCMX).

El Reglamento General de Protección de Datos Personales (en adelante Reglamento europeo) define los datos personales *sensibles* como "categorías especiales" de estos y otorga a los Estados parte de la libertad en su regulación, sin que omita señalar que denotan aquellos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, datos genéticos y datos biométricos (tratados únicamente para identificar un ser humano), datos relativos a la salud, así como los datos relativos a la vida sexual u orientación sexual de una persona.[18]

5.1 Datos de salud

En México este tipo de información es considerada como dato personal sensible, expresamente la ley señala "estado de salud presente o futuro" (Art. 3.X LGPDPPSO). Si bien la ley armonizada de la Ciudad de México refiere lo mismo, por cuanto hace a la temporalidad de la información, sus lineamientos (Art. 39) manifiestan que el responsable no podrá llevar a cabo el tratamiento de datos personales cuando tengan como efecto la discriminación de los titulares por su estado de salud "presente, pasado o futuro".

Es destacable la normativa de avanzada por la que se caracteriza la Ciudad de México, para el caso concreto describe con precisión esta categoría y señala que conforman datos sobre la salud: el expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona (Art. 62.VIII Lineamientos LGPDPPSOCMX).

18 Artículo 4, apartados 13, 13 y 15; artículo 9 y considerando 51-56 del RGPD.

El Reglamento europeo desarrolla de manera más amplia los *datos personales relativos a la salud, como* aquellos que refieren la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.[19] Además, menciona lo mismo que la ley armonizada de la Ciudad de México, es decir, que en los datos personales de salud se deben incluir todos aquellos relacionados con el estado de salud del interesado que proporcionen información acerca de su estado *físico* o *mental* "pasado, presente o futuro".[20]

También precisa que el tratamiento de "categorías especiales" de datos personales, ósea los datos sensibles, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. El cual debe estar sujeto a medidas adecuadas y específicas con la finalidad de proteger los derechos y libertades de las personas físicas. Además señala que la *salud pública* se interpreta como todos los elementos relacionados con esta, concretamente el *estado de salud*, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud; así como las necesidades de asistencia sanitaria, los recursos asignados a ella, la puesta a disposición de dicha asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la misma, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.[21]

5.2 Datos genéticos

El Reglamento europeo señala que son los datos personales relativos a

19 Artículo 4, inciso 15 del Reglamento general de protección de datos (UE) 2016/679.
20 Considerando 35 RGPD.
21 Considerando 54 RGPD

las características genéticas heredadas o adquiridas de una persona física que proporcionen información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.[22]

La Declaración Internacional sobre los Datos Genéticos Humanos (en adelante DIDGH), de 16 de octubre de 2003, de la Comisión Nacional de Bioética de Naciones Unidas, establece expresamente que los datos genéticos podrán ser recolectados, tratados, utilizados y conservados, solamente con las siguientes finalidades (Art. 5 DIDGH):

1. Diagnóstico y asistencia sanitaria, lo cual incluye la realización de pruebas de cribado y predictivas.[23]
2. Investigación médica y otras formas de investigación científica, comprendidos los estudios epidemiológicos, en especial los de genética de poblaciones, así como los estudios de carácter antropológico o arqueológico, que en lo sucesivo se designarán colectivamente como "investigaciones médicas y científicas".
3. Medicina forense y procedimientos civiles o penales u otras actuaciones legales, como las pruebas de determinación de parentesco, que se sujetarán a la legislación interna que sea compatible con el derecho internacional relativo a los derechos humanos (art. 1.c DIDGH).
4. Cualesquiera otros fines compatibles con la Declaración Universal sobre el Genoma Humano de 1997 (en adelante DUGH) y los Derechos Humanos y el derecho internacional relativo a los derechos humanos.

22 Artículo 4, inciso 13 del Reglamento general de protección de datos (UE) 2016/679.

23 Cribado genético: prueba genética sistemática que se realiza a gran escala y se ofrece como parte de un programa a una población o a un subconjunto de ella con el fin de detectar rasgos genéticos en personas asintomáticas (Art. 2.xiii DIDGH).

La Declaración sobre el genoma establece en su artículo 6 que nadie podrá ser objeto de discriminaciones fundadas en sus características genéticas, cuyo objeto o efecto sería atentar contra sus derechos y libertades fundamentales, así como el reconocimiento de su dignidad (art. 6 DUGH). En este sentido, solo la legislación de cada Estado podrá limitar los principios de consentimiento y confidencialidad, de haber razones imperiosas para ello, y a reserva del estricto respeto del derecho internacional público y del derecho internacional relativo a los derechos humanos (art. 9 DUGH).

En Europa existen dos tipos de bases de datos genéticos relacionados con perfiles de ADN. Por un lado están aquellas que se usan para las investigaciones criminales, cuyas muestras se recaban en escenas del crimen; y las que no se usan por la policía para esos fines, sino que son utilizadas para la búsqueda de personas desaparecidas, y sus muestras se obtienen directamente de la familia ascendente.[24]

a) Datos genéticos humanos

Estos conforman información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos[25] u otros análisis científicos (art. 2.i DIDGH). Asimismo, la Declaración refiere que la información genética forma parte del acervo general de los datos médicos y estos, a su vez, de los datos sensibles. Por lo tanto, en este caso, se desprende una *relación directa* de los datos genéticos, como datos de

24 Angers A, Kagkli DM, Oliva L, Petrillo M, Raffael B, Study on DNA Profiling Technology for its Implementation in the Central Schengen Information System, EUR 29766, Luxembourg: Publications Office of the European Union, 2019.

25 Los ácidos nucleicos son un tipo importante de macromoléculas presentes en todas las células y virus. Las funciones de los ácidos nucleicos tienen que ver con el almacenamiento y la expresión de información genética. El ácido desoxirribonucleico (ADN) codifica la información que la célula necesita para fabricar proteínas. Un tipo de ácido nucleico relacionado con él, llamado ácido ribonucleico (ARN), presenta diversas formas moleculares y participa en la síntesis de las proteínas, disponible en <https://www.genome.gov/es/genetics-glossary/acido-nucleico> (Consulta: 04/09/2021).

salud, y debido a ello resultan sensibles, *situación que no es igual para los datos biométricos pues no necesariamente son datos de salud*.

b) Muestra biológica

Los ácidos nucleicos se pueden obtener de una *muestra biológica* que conforma cualquier sustancia biológica (sangre, piel, células óseas o plasma sanguíneo) que albergue estos ácidos y contenga la dotación genética característica de una persona (art. 2.iv DIDGH).

c) Estudio de genética

Este puede emplearse para analizar *poblaciones* o el *comportamiento*, en el primer caso tiene por objeto entender la naturaleza y magnitud de las variaciones genéticas dentro de una población o entre individuos de un mismo grupo o de grupos distintos (art. 2.v DIDGH); mientras que el segundo, se refiere a aquel que tiene por objeto determinar las posibles conexiones entre los rasgos genéticos y el comportamiento (art. 2.vi DIDGH).

La Declaración señala algo sumamente importante para, cuando menos, dudar sobre categorizar los datos genéticos dentro del apartado de los datos biométricos. Al respecto, establece que cada individuo posee una configuración genética particular. Sin embargo, la *identidad de una persona* no debería reducirse a sus rasgos genéticos, pues en ella influyen complejos factores educativos, ambientales y personales, así como lazos afectivos, sociales, espirituales y culturales de esa persona con otros seres humanos, que conlleva además una dimensión de libertad (art. 3 DIDGH).

El Grupo de Trabajo 29 señaló que no necesariamente los datos genéticos constituyen datos biométricos. Pero, al respecto, señala la particularidad del carácter dual que tiene el ADN, pues además de proporcionar información sobre el cuerpo humano, permite la identificación inequívoca de una única persona.

D) Singularidad de los datos genéticos

Los datos genéticos son singulares porque: *1)* pueden indicar predisposiciones genéticas de las personas; *2)* pueden tener para la familia consecuencias importantes que se perpetúen durante generaciones, esto para la descendencia, y a veces para todo el grupo al que pertenezca la persona en cuestión; *3)* pueden contener información cuya relevancia no se conozca necesariamente en el momento de extraer las muestras biológicas; *4)* pueden ser importantes desde el punto de vista cultural para las personas o los grupos. La Declaración señala expresamente que se debería dar la debida atención al carácter *sensible* de los datos genéticos humanos e instituir un nivel de protección adecuado de éstos y de las *muestras biológicas* (art. 4 DIDGH).

Respecto a este tema, destaca la publicación de la "Ley por la que se crea el banco de ADN para uso forense de la Ciudad de México", el 24 de diciembre de 2019. En su artículo primero señala que tiene por objeto:

> I. Crear y regular el Banco de Perfiles Genéticos para uso forense del ADN de la Ciudad de México a fin de esclarecer hechos que puedan constituir los delitos de homicidio, lesiones, privación de la libertad personal con fines sexuales, incesto, secuestro, violación, estupro, privación ilegal de la libertad y feminicidio, con la finalidad de lograr la identificación de las personas responsables.

II. Establecer las bases de datos con la información genética de personas procesadas por la comisión de los delitos previstos.

III. Establecer las bases de datos con la información genética de las personas servidoras públicas que forman parte de las instituciones de seguridad ciudadana y de los integrantes del Gabinete de Seguridad Ciudadana y Procuración de Justicia, de la persona titular de la Jefatura de Gobierno y de los prestadores de los servicios de seguridad privada.

IV. Establecer la base de datos con la información genética de las víctimas de delitos de secuestro, violación, estupro, y feminicidio.

E) Algunas menciones en normas mexicanas

Al prinicipio de este análisis, se hacía mención de la poca regulación con la que cuenta México y que solo en algunas ocasiones se puede encontrar alguna vaga referencia, como por ejemplo:

1. El Reglamento de la Ley General de Salud en Materia de Trasplantes, contempla las siguientes menciones:

   Artículo 2. Para efectos del presente Reglamento, además de las definiciones previstas en el artículo 314 de la Ley, se entenderá por:

   Compatibilidad: El grado de semejanza *genética* entre los individuos que se comprueba después de llevar a cabo los estudios correspondientes a grupo sanguíneo, *inmunogenética*, antropometría o aquellos necesarios, atendiendo al órgano, tejido o célula de que se trate y al avance científico; que prevenga el riesgo de rechazo del órgano, tejido o células trasplantadas;

Histocompatibilidad: La semejanza entre dos o más Tejidos a nivel de sus características *genéticas* e inmunológicas; (cursivas propias)

2. La Ley de la Fiscalía General de la República, considera las siguientes menciones:

Artículo 38. La Fiscalía General diseñará, construirá y administrará un sistema informático nacional interoperable, alimentado en conjunto con las procuradurías y fiscalías de las entidades federativas del país, con el propósito de compartir información sobre datos existentes en las investigaciones, fenómenos y mercados criminales, características delictivas relevantes, incidencia, reincidencia, resoluciones y criterios relevantes, sanciones, reparación del daño y casos de éxito; así como toda la información relativa a registros y análisis de *perfiles genéticos* de personas, vestigios biológicos, huellas de individuos, huella balística, análisis de voz, *sistemas biométricos*, de vehículos y otros elementos relacionados con hechos delictivos, para la investigación (cursivas propias).

Artículo 40.XI.e Garantizar a las personas víctimas o sus familiares, la consulta de la *información genética* de sus familiares resguardada en las bases de datos que conforman el Banco Nacional de Datos Forenses, para la identificación de cuerpos o restos humanos, en el caso de personas desaparecidas, de conformidad con lo que establezcan los Lineamientos Generales en esta materia (cursivas propias).

Artículo 42.XI Operar junto con la unidad administrativa correspondiente un sistema informático de registro y análisis de la huella balística, análisis de voz, sistemas biométricos, *información genética* y otros elementos relacionados con hechos delictivos, que se obtengan de conformidad con las disposiciones aplicables, así como compartir la información con unidades específicas del Ministerio Público, de la Policía Federal Ministerial y de información y análisis (cursivas propias).

5.3 Datos biométricos

Los datos biométricos son definidos por el Reglamento europeo, como aquellos obtenidos a partir de un tratamiento técnico específico, relativos a características físicas, fisiológicas o conductuales de una *persona física* que permitan o confirmen la identificación única como imágenes faciales o datos dactiloscópicos.[26]

Es de señalar nuevamente el dictamen de la Comisión de Transparencia y Anticorrupción de la Cámara de Diputados de México, aprobado el 3 de febrero de 2021, para considerar datos sensibles aquella información genética *o biométrica dirigida a identificar de manera unívoca a una persona física*.[27]

El Grupo de Trabajo del Artículo 29, precisa que los datos de salud no son datos biométricos, como tampoco lo sería una muestra de tejido humano. Pero que el ADN tiene un carácter dual, pues además de ser un dato genético, también conforma un dato biométrico.[28]

26 Artículo 4, inciso 14 del RGPD (UE) 2016/679.

27 Referencia en el apartado "5. Datos Sensibles" de este mismo documento. Cámara de Diputados. Legislatura XXIV. *Gaceta Parlamentaria*, año XXIV, núm. 5709_VI. Disponble en <http://gaceta.diputados.gob.mx/PDF/64/2021/feb/20210203-VI.pdf> (Consulta: 25/09/2021). Las definiciones de la Real Academia Española son 1) Creencia: i) firme asentimiento y conformidad con algo, ii) completo crédito que se presta a un hecho o noticia como seguros o ciertos, iii) religión, doctrina; 2) Convicción: i) convencimiento, ii) idea religiosa ética o política a la que se está fuertemente adherido; 3) Preferencia: i) primacía, ventaja o mayoría que alguien o algo tiene sobre otra persona o cosa, ya en el valor, ya en el merecimiento; ii) elección de alguien o algo entre varias personas o cosas; 4) Orientación: acción y efecto de orientar u orientarse; 4.1) Orientar: dar a alguien información o consejo en relación con un determinado fin; 5) Genético, ca: parte de la biología que trata de la herencia y de lo relacionado con ella; 5.1) Información genética: conjunto de mensajes codificados en los ácidos nucleicos que origina la expresión de los caracteres hereditarios propios de los seres vivos mediante reacciones bioquímicas; 6) Biométrico, ca: perteneciente o relativo a la biometría; 6.1) Biometría: estudio mensurativo o estadístico de los fenómenos o procesos biológicos.

28 Dictamen 4/2007 sobre el concepto de datos personales, del Grupo de Trabajo del Artículo 29, adoptado el 20 de junio.

II. LOS DATOS BIOMÉTRICOS

Estos se relacionan con aquella información que mide el cuerpo de una persona y que la hace única e identificable respecto de otras. Los riesgos de la privacidad de las personas, a través de la vulneración de los datos biométricos, comenzaron a formar parte de la preocupación colectiva luego de que la vida diaria se digitalizó, acción que se incrementó con la situación de encierro y distanciamiento social provocado por la pandemia de Covid19.

En México durante el año 2021 el tema eferveció a partir de la propuesta de reforma a la Ley Federal de Telecomunicaciones y Radiodifusión (en adelante LFTR), con la creación del Padrón Nacional de Usuarios de Telefonía Móvil (en adelante PANAUT), que recaba datos personales, incluidos los biométricos.

1. Biometría

Este concepto denota la medición del cuerpo para identificar y reconocer a una persona. La Organización para la Cooperación y el Desarrollo Económico (en adelante OCDE) ha señalado que consiste en características únicas y medibles de rasgos, físicos o de comportamiento, en los seres humanos que sirven para *automáticamente* reconocer o verificar una identidad. La técnica surge a partir de la materia de seguridad y criminalística para identificar a quienes hubiesen cometido un delito.[29]

Los lineamientos de la LPDPPSOCDMX establecen que la biometría es el análisis técnico específico para el reconocimiento inequívoco de personas, basado en uno o más rasgos conductuales o físicos intrínsecos mediante el uso de dispositivos y sistemas electrónicos (art. 2.II).

29 OECD (2004-06-30), "Biometric-based Technologies", *OECD Digital Economy Papers*, No. 101, OECD Publishing, Paris.

2. Datos biométricos

Como ya se ha establecido, son definidos por el Reglamento europeo como aquellos obtenidos a partir de un tratamiento técnico específico, relativos a características físicas, fisiológicas o conductuales de una *persona física* que permitan o confirmen la identificación única como imágenes faciales o datos dactiloscópicos.[30]

El Grupo de Trabajo del Artículo 29 lleva a cabo un análisis importante sobre el tema al definir los datos biométricos como aquellas propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics nerviosos, que resultan atribuibles a *una sola persona* y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad.[31]

El dictamen cita además como ejemplos típicos de datos biométricos los que proporcionan las huellas dactilares, los modelos retinales, la estructura facial, las voces, aunque también la geometría de la mano, las estructuras venosas e inclusive determinada habilidad profundamente arraigada u otra característica del comportamiento como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etcétera.

a) El carácter dual del ADN

El Dictamen del Grupo de Trabajo del Artículo 29 señala que los datos de salud no son datos biométricos, como tampoco lo sería una muestra de tejido humano. También refiere que los datos genéticos, si bien constituyen datos de salud, no necesariamente son biométricos (como se ha explicado en páginas anteriores).

Sin embargo, establece que el ADN tiene un carácter dual, pues además

30 Artículo 4, inciso 14 del Reglamento general de protección de datos (UE) 2016/679.
31 Dictamen 4/2007 de 20 de junio, sobre el concepto de datos personales del Grupo de Trabajo del Artículo 29.

de ser un dato genético, también es biométrico.[32] El dictamen indica que una particularidad de los datos biométricos establece que se les puede considerar tanto a) *contenido* de la información sobre una determinada persona, por ejemplo: Luis tiene estas huellas dactilares; y b) como *elemento para vincular* una información a una determinada persona, por ejemplo: este objeto lo ha tocado alguien que tiene estas huellas dactilares y estas corresponden a Luis, por lo tanto Luis ha tocado este objeto. Como tales, pueden servir de "identificadores". En este sentido, al corresponder a una única persona, los datos biométricos pueden utilizarse para identificar a dichaa persona. Este carácter dual, señala el Grupo de Trabajo, por igual, se da en el caso de datos sobre el ADN, que proporcionan información del cuerpo humano y permiten la identificación inequívoca de una solo persona.

b) Características

El Instituto Nacional de Acceso a la Información y Protección de Datos Personales (en adelante INAI) refiere que los datos biométricos tienen cuatro características particulares, a saber:[33]

1. Universales, ya que son datos con los que cuentan todas las personas.
2. Únicos, porque no existen dos biométricos con las mismas características por lo que aquellos de una persona se distinguen de otras.
3. Permanentes, pues se mantienen, en la mayoría de los casos, a lo largo del tiempo en cada persona.
4. Medibles, dan forma cuantitativa.

En este sentido, para que un dato sea considerado biométrico debe de ser universal pues se consideran propios a toda persona, es único debido

32 Dictamen 4/2007 sobre el concepto de datos personales, del Grupo de Trabajo del Artículo 29, adoptado el 20 de junio.

33 INAI (2018). *Guía para el Tratamiento de Datos Biométricos*.

a que distingue sin error alguno a una persona de otra, es permanente porque permanece en la persona a lo largo de su vida y se puede medir de manera cuantitativa.

c) Descripción de datos biométricos

La *Guía para el Tratamiento de Datos Biométricos,* publicada por el Instituto Nacional de Acceso a la Información y Protección de Datos Personales, describe de manera útil algunos de estos datos, dividiéndolos en dos grandes categorías; que conforman aquellos que se refieren a las medidas biológicas y los relacionados con las características de comportamiento y personalidad.

Ejemplos de datos biométricos que corresponden a *características biológicas*, los cuales permiten la identificación o autenticación de una persona.

Biométrico	Descripción de reconocimiento
Huella dactilar	Es la más antigua y existen dos técnicas: (i) Basada en minucias y (ii) basada en correlación. Esta última requiere un registro más preciso pues se analiza el patrón global seguido por la huella dactilar.
Reconocimiento facial	El análisis se realiza a través de mediciones como la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula.
Reconocimiento de iris	Una cámara infrarroja escanea el iris y proporciona sus detalles. Los patrones del iris vienen marcados desde el nacimiento y rara vez cambian, son muy complejos y contienen una gran cantidad de información, más de 200 propiedades únicas.
Geometría de la mano	A través de una cámara se captura imágenes en 3-D, se extraen características que incluyen las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano, las distancias entre las articulaciones y la estructura ósea.
Reconocimiento de retina	Se basa en la utilización del patrón de los vasos sanguíneos contenidos en la misma. Cada patrón es único incluso entre los gemelos idénticos y tiene una tasa de falsos positivos prácticamente nula.
Reconocimiento vascular	Se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo. Es interno y no deja rastro por lo que el robo de identidad es muy difícil.

Fuente: Elaboración del INAI.[34]

Ejemplos de datos biométricos que corresponden a *características de comportamiento y personalidad*, las cuales permiten la identificación de una persona.

Biométrico	Descripción de reconocimiento
Reconocimiento de firma	Analiza la firma autógrafa o manuscrita para confirmar la identidad del firmante. Existen dos variantes: (i) Comparación simple, que considera el grado de parecido entre dos firmas, y (ii) verificación dinámica, que hace un análisis de la forma, velocidad, presión de la pluma y la duración del proceso de firma.
Reconocimiento de escritura	Se vale de un software de reconocimiento de caracteres, atendiendo a que cada persona tiene una forma de escribir diferente, teniendo rasgos propios e inconfundibles para cada letra. De igual forma, cada persona tiene un grado de inclinación y nivel de presión al escribir.
Reconocimiento de voz	Se usan sistemas de inteligencia artificial con algoritmos que deben medir y estimar la similitud entre las muestras para devolver un resultado o una lista de posibles candidatos.

34 *Ídem*.

Reconocimiento de escritura de teclado	Se basa en el hecho de la existencia de un patrón de escritura en el teclado permanente y propio de cada individuo, por lo que un software mide la fuerza de tecleo, la duración de la pulsación y el periodo que pasa entre que se presiona una tecla y otra.
Reconocimiento de la forma de andar	Se graba la forma de caminar de una persona y se somete a un proceso analítico que genera una plantilla biométrica única. Se encuentra aún en desarrollo y no tiene los mismos niveles de rendimiento que otras tecnologías biométricas.

Biométrico	Descripción de reconocimiento
Reconocimiento de escritura de teclado	Se basa en el hecho de la existencia de un patrón de escritura en el teclado permanente y propio de cada individuo, por lo que un software mide la fuerza de tecleo, la duración de la pulsación y el periodo que pasa entre que se presiona una tecla y otra.
Reconocimiento de la forma de andar	Se graba la forma de caminar de una persona y se somete a un proceso analítico que genera una plantilla biométrica única. Se encuentra aún en desarrollo y no tiene los mismos niveles de rendimiento que otras tecnologías biométricas.

Fuente: Elaboración del INAI.[35]

3. Algunas menciones en la legislación mexicana

Se hace mención de la poca regulación con la que cuenta México para los datos genéticos, pues la situación de los biométricos es también escasa, vaga e incluso las referencias se encuentran de manera indirecta al mencionar la huella dactilar (abona a la confusión el uso del sinónimo *huella digital*), fotografía, etnia, etcétera. Algunas referencias se pueden encontrar por ejemplo, en los siguientes instrumentos normativos:

1. La Ley General de Salud, contempla la siguiente mención:

   Artículo 53 Bis. Los prestadores de servicios de salud, para efectos de identificación de usuarios de los servicios de salud, incluyendo los derechohabientes de los organismos de seguridad social, podrán implementar *registros biométricos* y otros medios de identificación electrónica (cursivas propias).

2. La Ley de la Fiscalía General de la República, contempla las siguientes menciones:

35 *Ídem.*

Artículo 38. La Fiscalía General diseñará, construirá y administrará un sistema informático nacional interoperable, alimentado en conjunto con las procuradurías y fiscalías de las entidades federativas del país, con el propósito de compartir información sobre datos existentes en las investigaciones, fenómenos y mercados criminales, características delictivas relevantes, incidencia, reincidencia, resoluciones y criterios relevantes, sanciones, reparación del daño y casos de éxito; así como toda la información relativa a registros y análisis de perfiles genéticos de personas, vestigios biológicos, *huellas de individuos*, huella balística, análisis de *voz*, *sistemas biométricos*, de vehículos y otros elementos relacionados con hechos delictivos, para la investigación (cursivas propias).

Artículo 42.XI Operar junto con la unidad administrativa correspondiente un sistema informático de registro y análisis de la huella balística, análisis de voz, *sistemas biométricos*, información genética y otros elementos relacionados con hechos delictivos, que se obtengan de conformidad con las disposiciones aplicables, así como compartir la información con unidades específicas del Ministerio Público, de la Policía Federal Ministerial y de información y análisis (cursivas propias).

3. La Ley General del Sistema Nacional de Seguridad Pública, contempla las siguientes menciones:

Artículo 5.II.- Para los efectos de esta Ley, se entenderá por: Bases de Datos aquellas que constituyen subconjuntos sistematizados de la información contenida en Registros Nacionales en materias relativas a detenciones, armamento, equipo y personal de seguridad pública, medidas cautelares, soluciones alternas y formas de terminación anticipada, así como las bases de datos del Ministerio Público y las instituciones policiales de los tres órdenes de gobierno relativas a la información criminalística, *huellas dactilares* de personas sujetas a un proceso o investigación penal, teléfonos

celulares, personas sentenciadas y servicios de seguridad privada, así como las demás necesarias para la prevención, investigación y persecución de los delitos. El conjunto de bases de datos conformará el Sistema Nacional de Información (cursivas propias).

Artículo 42.- El documento de identificación de los integrantes de las instituciones Seguridad Pública deberá contener al menos nombre, cargo, fotografía, *huella digital* y clave de inscripción en el Registro Nacional de Personal de Seguridad Pública, así como, las medidas de seguridad que garanticen su autenticidad (cursivas propias).

Artículo 110.- Los integrantes del Sistema están obligados a permitir la interconexión de sus Bases de Datos para compartir la información sobre Seguridad Pública con el Sistema Nacional de Información, en los términos de esta Ley y otras disposiciones jurídicas aplicables. Para ello, se adoptarán los mecanismos tecnológicos necesarios para la interconexión en tiempo real y respaldo de la información.

La información contenida en las Bases de Datos del Sistema Nacional de Información, podrá ser certificada por la autoridad respectiva y tendrá el valor probatorio que las disposiciones legales determinen. Se clasifica como reservada la información contenida en todas y cada una de las Bases de Datos del Sistema Nacional de Información, así como los Registros Nacionales y la información contenida en ellos, en materia de detenciones, información criminal, personal de seguridad pública, personal y equipo de los servicios de seguridad privada, armamento y equipo, vehículos, *huellas dactilares*, teléfonos celulares, medidas cautelares, soluciones alternas y formas de terminación anticipada, sentenciados y las demás necesarias para la operación del Sistema (cursivas propias).

Artículo 122.- El Registro Nacional de Personal de Seguridad Pública es la Base de Datos que, dentro del Sistema Nacional de

Información y conforme lo acuerden las Conferencias Nacionales de Procuración de Justicia y de Secretarios de Seguridad Pública, contendrá la información actualizada, relativa a los integrantes de las Instituciones de Seguridad Pública de la .Federación, las entidades federativas y los Municipios, el cual contendrá, por lo menos: I. Los datos que permitan identificar plenamente y localizar al servidor público, sus *huellas digitales*, fotografía, escolaridad y antecedentes en el servicio, así como su trayectoria en la seguridad pública (cursivas propias).

4. La Ley de la Policía Federal, contempla la siguiente mención:

Artículo 7. XLIV. Integrar en el Registro Administrativo de Detenciones y demás bases de datos criminalísticos y de personal, las *huellas decadactilares* y otros elementos distintos a las fotografías y videos para identificar a una persona, solicitando a las autoridades de los tres órdenes de gobierno la información respectiva con que cuenten (cursivas propias).

5. La Ley Nacional del Registro de Detenciones, señala lo siguiente:

Artículo 23. La actualización de la información del Registro que lleven a cabo las instituciones de procuración de justicia o administrativas deberá contener, cuando menos, los datos de la persona detenida, que serán: a) Lugar y fecha de nacimiento; b) Domicilio; c) Nacionalidad y lengua nativa; d) Estado civil; e) Escolaridad; f) Ocupación o profesión; g) Clave Única de Registro de Población; h) *Grupo étnico* al que pertenezca; i) Descripción del estado físico de la persona detenida y nombre del médico que certificó o, en su caso, copia del certificado médico; j) *Huellas dactilares*; k) *Fotografía* de la persona detenida, y l) Otros medios que permitan la identificación plena de la persona (cursivas propias).

4. Normativas locales de protección de datos personales

Las leyes locales de las entidades federativas se encuentran a la fecha armonizadas con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, si bien esta no prevé la mención de los *datos biométricos* dentro de la categoría de *datos sensibles*, si resulta posible localizarla en algunas leyes locales de protección de datos personales. Por ejemplo, se puede encontrar la mención de "datos biométricos" en la ley de la materia de: Campeche (art. 3.X), Chiapas (art. 5.IX), Chihuahua (art. 11.IX), Ciudad de México (arts. 3.X y 25.III), Guanajuato (art. 3.X), Guerrero (art. 3.VIII), Hidalgo (art. 3. VIII), Estado de México (art. 43.B.III), Morelos (art. 38.B.III), Nuevo León (art. 3.XI), Puebla (art. 5.IX), Quintana Roo (art. 4.XI), San Luis Potosí (art. 3.IX), Sonora (art. 3.VIII), Tamaulipas (art. 3.VIII), Tlaxcala (art. 10.III), Veracruz (art. 43.B.III), Zacatecas (arts. 3.VIII.b, 15 y 37.B.III) y Jalisco (art. 3.X).[36]

Es ejemplar la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Zacatecas, pues su normativa representa la única entre las 34 leyes de protección de datos personales de todo el país que define expresamente los datos biométricos como aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población. Además, refiere de manera detallada, en esta categoría de datos: las huellas dactilares, geometría de la mano, análisis del iris y retina, venas del dorso de la mano, rasgos faciales, patrón de voz, firma manuscrita, dinámica de tecleo, cadencia del paso al caminar, análisis gestual y del ADN (art. 3.VIII.b).[37]

36 En el resto de las entidades federativas no se encontró mención alguna, ni en la categorización de datos sensibles, ni tampoco en su tratamiento o medidas de seguridad.
37 Se consideran 34 leyes pues son 2 nacionales y 32 de las entidades federativas.

5. PANAUT 2021

En México, durante el mes de abril del 2021, el tema eferveció a partir de la reforma a la Ley Federal de Telecomunicaciones y Radiodifusión, que crea el Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT), el cual recaba datos personales, incluidos los biométricos.[38]

Luego el 13 de mayo del mismo año, el INAI promovió la Acción de Inconstitucionalidad 82/2021, solicitando a la Suprema Corte de Justicia de la Nación suspender todos los efectos de la reforma de la citada ley, para evitar que se entreguen datos personales de los usuarios de telefonía móvil, considerando que se violan los derechos de privacidad, intimidad, protección de los datos personales, interés superior del menor e identidad.

A continuación se describe, de manera breve, el contenido del dictamen por el que se reforma la Ley Federal de Telecomunicaciones y Radiodifusión.[39]

5.1 Objetivo

La reforma busca inhibir en su totalidad los principales delitos que aquejan a la sociedad mexicana, y que se cometen a través del uso de equipos móviles como herramienta para la realización de distintos ilícitos. Estos se llevan a cabo a través de servicios de voz, buzón vocal, conferencia y datos, así como el reenvío o transferencia de llamada o servicio de mensajería. En México, el delito de extorsión se hace principalmente a través del engaño telefónico, la amenaza telefónica y el cobro de derecho de piso.

38 Publicada el 16 de abril de 2021 en el *Diario Oficial de la Federación*.
39 Dictamen del Senado de la República, de fecha 25 de marzo de 2021, en sentido positivo de las comisiones unidas de comunicaciones y transportes; y de estudios legislativos, respecto a la minuta con proyecto de decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión.

El objetivo es la identificación plena y certera de los titulares de las líneas de comunicación, para identificar la comisión de un delito a través de equipos móviles debido a que hasta diciembre de 2019 había en México más de cien millones de líneas contratadas en la modalidad de prepago que no exige requisito alguno para la adquisición de una línea de telefonía móvil, abonando así al anonimato de las actividades ilícitas de la delincuencia como: extorsión, secuestro o cualquier otra operación criminal a través de la telefonía celular. La falta de controles en la identificación de los usuarios impide que las áreas de inteligencia de seguridad pública rastreen la geolocalización.

En este sentido, el Estado mexicano es quien tiene el deber de garantizar la seguridad pública y nacional, así como una efectiva procuración de justicia, a través de mandatos por escrito que deberán atender los concesionarios y autorizados. A su vez, el dictamen establece la importancia de que al día de hoy las empresas de telecomunicaciones tengan responsabilidad frente a sus usuarios, respecto a su seguridad personal, controlando y ubicando a las personas que contratan los servicios. Esto para identificar eficaz y eficientemente las comunicaciones en torno a delitos.

5.2 Contenido

El Padrón Nacional de Usuarios de Telefonía Móvil, a decir por el dictamen, contempla una base de datos con información de las personas físicas o morales titulares de cada línea telefónica móvil que cuenten con número del Plan Técnico Fundamental de Numeración y cuyo fin es el de colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos. El PANAUT contendrá (art. 180 Ter LFTR):

1. Número de línea telefónica móvil.
2. Fecha y hora de la activación de la línea telefónica móvil adquirido

en la tarjeta SIM.

3. Nombre completo o, en su caso, denominación o razón social del usuario.
4. Nacionalidad.
5. Número de identificación oficial con fotografía o Clave Única del Registro de Población del titular de la línea.
6. *Datos biométricos* del usuario y, en su caso, del representante legal de la persona moral, conforme a las disposiciones administrativas de carácter general que al efecto emita el Instituto (cursivas propias).
7. Domicilio del usuario.
8. Datos del concesionario de telecomunicaciones o, en su caso, de los autorizados.
9. Esquema de contratación de la línea telefónica móvil, ya sea pospago o prepago.
10. Los avisos que actualicen la información a que se refiere este artículo.

Lo discutible por la opinión pública y el INAI, al interponer la Acción de Inconstitucionalidad, fue la mención en general de "datos biométricos", sin precisar exactamente cuáles, como podría haber sido únicamente la huella dactilar o el reconocimiento facial. Resulta de suma importancia prestar atención sobre el dato que de manera eventual se solicite, pues este deberá ser protegido con las máximas medidas de seguridad y tendrá que ser el menos invasivo para la finalidad de su recolección, esto es, la de contratar una línea de telefonía móvil y con la finalidad de prevenir delitos graves.

5.3 Análisis

Con relación al Padrón Nacional de Usuarios de Telefonía Móvil es importante reflexionar sobre los siguientes puntos:

1. Las críticas al PANAUT están directamente relacionadas con el tratamiento de datos personales sensibles, como los biométricos, por elIo requiere que su estudio, análisis, regulación y posibles sanciones por el indebido tratamiento estén expresamente a cargo del órgano garante de protección de datos personales, es decir, el INAI. Más aún, cuando la propia reforma señala que la información contenida en el PANAUT será confidencial y reservada en los términos de la Ley General de Transparencia y Acceso a la Información Pública, de 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 Particulares.
2. El antecedente del PANAUT se encuentra en el Registro Nacional de Usuarios de Telefonía Móvil (RENAUT) de 2009,[40] que sería fundamental analizar a profundidad por lo que hace a su desarrollo, implementención y causas por las que no prosperó.
3. Otros instrumentos normativos en México contemplan la recolección y tratamiento de datos personales biométricos, aunque de forma más precisa mencionando la huella dactilar y/o la fotografía.
4. La preocupación de la sociedad se agravó pues representan millones los usuarios de telefonía móvil,[41] por lo tanto, la privacidad de todos ellos se pondría en riesgo al no contar con una regulación más detallada que expresara las garantías del derecho a la protec-

40 Publicado el 9 de enero de 2009 en el *Diario Oficial de la Federación*, por decreto en el que se reformó la Ley Federal de Telecomunicaciones y se creó el RENAUT. Luego en mayo del mismo año la Comisión Federal de Comunicaciones publicó las reglas de regulacion en las que se establecía como medio de identificación la Clave Única de Registro de Población (CURP). Este registro desaparece en 2011.

41 El anuario estadístico de 2019, a diciembre de ese año a nivel nacional, había 122 millones de líneas del servicio móvil de telefonía (83.5% de líneas prepago).

ción de datos personales, privacidad, identidad, etcétera.

5. México sufre un problema de inseguridad que, a través de la historia, cada año se agrava y normaliza (siempre ha sido así) por diversas circunstancias económicas, sociales, políticas, internacionales, entre otras. Por ello, es importante que el Estado pueda crear e implemetar nuevas formas de combate a la inseguridad, como los registros, padrones y bases de datos. Para ello es indispensable la *inversión en tecnología* con el objetivo de que sea posible el garantizar la debida protección de los derechos humanos como la *protección de los datos personales*, privacidad, identidad, integridad personal, libertad de tránsito, y todo lo demás.
6. Es posible que la historia de esta controvertida reforma hubiese sido otra, de haberse publicado con ella las disposiciones administrativas de las que habla la ley para el caso de recopilar datos biométricos.

III. PROTECCIÓN DE LOS DATOS BIOMÉTRICOS

Estos corresponden a aquella información que mide el cuerpo de una persona y que la hace única e identificable respecto de otras. Los riesgos de la privacidad de las personas, a través de la vulneración de los datos biométricos, comenzaron a formar parte de la preocupación colectiva luego de que la vida diaria se digitalizó, e incrementado por la situación de aislamiento y distanciamiento social, provocado por la pandemia de Covid-19.

1. Riesgos y medidas de prevención

Los riesgos y amenazas ante el tratamiento indebido de datos biométricos son variados, entre ellos se encuentra la conformación de bases de datos destinadas a la creación de *perfiles de la personalidad*, producto del almacenamiento de información personal sensible, por ejemplo, los perfiles de ADN. Estos, resultan muy útiles en el combate a la delincuencia, pues revelan la identidad de personas sospechosas de haber cometido un delito grave. Sin embargo, la deficiente regulación en esta materia, puede ocasionar que las bases de datos sean creadas para fines ajenos al bienestar social (persecusión de delitos); y, por el contrario, se vulneren derechos humanos como la privacidad, intimidad, identidad, igualdad, integridad personal, libre desarrollo de la personalidad, etcétera.

Para prevenir riesgos es importante minimizar el uso y recopilación de los datos biométricos. Es decir, el responsable del tratamiento deberá solicitar solo los datos necesarios para la finalidad o trámite correspondiente, y la persona titular de los datos deberá estar atenta para no entregar datos personales que excedan de los estrictamente requeridos para

tal fin, en otras palabras, que la información solicitada no sea mayor e innecesaria para el objetivo del trámite.

Asimismo, el periodo de conservación de la información personal debe de ser limitado y después deberá de ser cancelada o destruida. Cabe destacar que está estrictamente prohibido realizar bases de datos destinadas sólo para recabar información personal sensible, creación de perfiles personales que se utilicen para segregar, clasificar o discriminar a las personas en modo alguno.

El INAI recomienda proporcionar la menor cantidad posible de datos biométricos, más aún cuando es optativo o una forma secundaria de autenticación:

Fuente: Secretaría de Datos Personales del INAI.

2. Derechos ARCO

Para una correcta protección de los datos personales en general, de manera especial los datos biométricos, esta prerrogativa contiene un haz de facultades que son los derechos ARCO, acrónimo que refleja las iniciales de los derechos de acceso, rectificación, cancelación y oposición. Con la LGPDPPSO se adiciona un derecho más que corresponde al de portabilidad, por lo tanto, cabe la posibilidad de decir que el acrónimo cambia de ARCO a ARCOP.

Los medios para ejercer los derechos ARCO se encuentran en el aviso de privacidad, por ello la importancia de leerlo cada vez que se proporcionan datos personales. También, por eso la obligación que tiene el responsable del tratamiento de datos de disponer el aviso de privacidad de modo público y accesible para los titulares de la información, quienes a su vez tienen el derecho de conocer dicha advertencia.

El segundo capítulo de la Ley establece que la recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO que se formulen a los responsables (dependencia pública, tienda, banco, gimnasio, etc.) será gratuito y se sujetará al procedimiento establecido. Para ello, será necesario acreditar la identidad del titular y, en su caso, también la personalidad con la que actúe el representante.[42]

Cuando ocurre la vulneración de datos personales, de cualquier tipo, ya sean sensibles o no, los pasos a seguir son los siguientes:

1) Consultar el aviso de privacidad del responsable e identificar el trámite previsto para presentar una solicitud de ejercicio de derechos ARCO. En este se encuentra la dirección física y/o correo electrónico en el que se deberá entregar dicha solicitud.

42 En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación. Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere la ley, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto.

2) La solicitud de derechos ARCO se presenta *ante el responsable* (banco, tienda departamental, gimnasio, dependencia pública, etc.) del que se sospecha o haya vulnerado los datos personales.

3) Si el responsable no atendió la solicitud de la forma esperada, entonces se podrá presentar el Recurso de Revisión ante el órgano garante. Atendiendo a las siguientes consideraciones:

   a. Ante el INAI. Cuando quien vulnera los datos personales sea una *institución de carácter privado*, ubicada en cualquier entidad federativa de México, por ejemplo: una tienda departamental, banco, gimnasio, etcétera.

   b. Ante el INAI. Cuando quien vulnera los datos personales sea una *dependencia pública federal*, por ejemplo, Secretaría de Economía, Secretaría de Educación, Secretaría de Gobernación, UNAM, INAI, INE, Tribunal Electoral de la Federación, etcétera.

   c. Ante el InfoCDMX o cualquier órgano garante local de las entidades federativas. Cuando quien vulnera los datos personales sea una *dependencia pública local*, como puede ser para el caso de la Ciudad de México, Secretaría de Desarrollo Urbano y Vivienda, Secretaría de Inclusión y Bienestar Social, Secretaría de Movilidad, Secretaría de las Mujeres, Secretaría de Salud, Secretaría de Pueblos y Barrios Originarios y Comunidades Indígenas Residentes, etcétera.

a) Plazos

El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO, cuyo plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud; que podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias. En caso de resultar pro-

cedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta al titular (art. 51 LGPDPPSO).

b) Requísitos

En la solicitud para el ejercicio de los derechos ARCO no podrán imponerse mayores requisitos que los siguientes: a) El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones; b) Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante; c) De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud; d) La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso; e) La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y f) Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso (art. 52 LGPDPPSO).

c) Modalidad de entrega

Tratándose de una solicitud de acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que estos se reproduzcan. El responsable tendrá que atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en la misma, en este caso deberá ofrecer otras alternativas de entrega de los datos personales fundando y motivando dicha actuación (art. 52 LGPDPPSO).

d) Lugar de entrega

Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del responsable, que el titular considere competente, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto y los organismos garantes, en el ámbito de sus respectivas competencias (art. 52 LGPDPPSO). Cabe destacar la herramienta de la Plataforma Nacional de Transparencia (PNT), una página web en la que es posible consultar las obligaciones de transparencia y realizar las solicitudes de acceso a la información y protección de datos personales.

2.1 Constitución Política de los Estados Unidos Mexicanos

La Constitución mexicana garantiza la protección de los datos personales en sus artículos 6 y 16. A saber, el art. 6.A.II.l establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Luego, el art. 16 refiere 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.

2.2 Ley Federal de Protección de Datos Personales en Posesión de Particulares

Los derechos ARCO, según esta Ley, se pueden definir de la siguiente forma:

1. Acceso: las personas 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 (art. 23).
2. Rectificación: el titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos (art. 24).
3. Cancelación: el titular tendrá en todo momento el derecho a cancelar sus datos personales. Esta 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. Una vez cancelado el dato se dará aviso a su titular. Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también (art. 25).
4. Oposición: la persona 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 (art. 27).
5. Portabilidad: esta Ley de 2010 no contempla el derecho de portabilidad de los datos personales, pues es más antigua que la LPDPPSO, que al ser más reciente contempla muchos otros supuestos de prevención, garantía y protección del derecho a la protección de datos personales en posesión de sujetos obligados.

2.3 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Los derechos ARCO, según esta Ley, se pueden definir de la siguiente forma:

1. Acceso: la persona titular de la información tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento (art. 44 LGPDPPSO).
2. Rectificación: el titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados (art. 45 LGPDPPSO).
3. Cancelación: El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último (art. 46 LGPDPPSO).
4. Oposición: El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando: I. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y II. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento (art. 47 LGPDPPSO).
5. Portabilidad: Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular

tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico generalmente usado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales (art. 57 LGPDPPSO).

Conclusión

Los datos personales son cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Los datos biométricos constituyen aquellos obtenidos a partir de un tratamiento técnico específico, relativos a características físicas, fisiológicas o conductuales de una *persona física* que permitan o confirmen la identificación única como imágenes faciales o datos dactiloscópicos.

La protección de los datos personales, especialmente los sensibles, entre los que destacan los datos biométricos, es responsabilidad –en primera instancia– de cada persona titular de los mismos, y proporcionar solamente aquellos que sean estrictamente necesarios para el trámite que se realiza. Luego, es obligación del Estado garantizar efectivamente el desarrollo de políticas públicas y el debido cumplimiento de las leyes que garantizan a la ciudadanía la protección de este derecho humano.

La pandemia del virus SARS-COV2, originó el distanciamiento social, provocando que la totalidad de las actividades diarias se realizaran a través de las TIC. Por ello, los órganos garantes de transparencia del país, tanto el nacional como los locales, se volcaron en un trabajo enorme de difusión de medidas para prevenir los riesgos en internet y las aplicaciones móviles, producto de la vulneración de datos personales.

Cuando una persona sospecha sobre la posible vulneración del derecho a la protección de datos personales, esta deberá acudir ante el responsable (banco, gimnasio, dependencia pública, tienda departamental, etc.) y consultar el aviso de privacidad, que indicará la información necesaria para presentar una solicitud de datos personales y ejercer alguno de los derechos ARCO. Una vez recibida la respuesta a dicha solicitud, si la persona no se está de acuerdo o bien el responsable no atendió la petición,

se deberá acudir al órgano garante nacional o local, según corresponda, para presentar un Recurso de Revisión en contra de la respuesta.

Es importante que cada persona sea responsable de su información personal, al momento de entregar sus datos, más aún si estos son sensibles, como los *datos biométricos*. En lo posible, cuando la entrega aparece opcional o secundaria, la recomendación es no entregarlos y optar por otro medio de autentificación.

Bibliografía

Monografías y artículos científicos

Angers A, Kagkli DM, *et al.* (2019) *Study on DNA Profiling Technology for its Implementation in the Central Schengen Information System*, EUR 29766, Luxembourg: Publications Office of the European Union.

Campuzano Tomé, H. (2000). *Vida privada y datos personales.* Madrid: Tecnos.

Conde Ortiz, C. (2005). *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad.* Madrid: Dykinson.

Fioriglio, G. (2008). *Il diritto a la privacy. Nuove frontiere nell'era di internet*. Bologa: Bologna University Press.

Garriga Domínguez, A. (2004). *Tratamiento de datos personales y derechos fundamentales.* Madrid: Dykinson.

González Pascual, M. (septiembre/diciembre de 2009). El Tribunal Constitucional Federal alemán ante la compatibilidad con los derechos fundamentales de la normativa nacional de origen europeo de prevención de delitos, en *Revista de Derecho Comunitario Europeo* (núm. 34, año 13), 945-966.

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

Martínez Martínez, R. (2004). *Una aproximación crítica a la autodeterminación informativa.* Madrid: Thomson-Civitas y APDCM.

Mattelart, A. (2001). *Historia de la sociedad de la información.* (G. Multigner, Trad.) París: Le Découverte.

OECD (2004). *Biometric-based Technologies*, *OECD Digital Economy Papers*, No. 101, OECD Publishing, Paris.

Ruiz de Querol, R., y Buira, J. (2007). *La sociedad de la información.* Barcelona: UOC.

Ruíz Miguel, C. (2004). *Estudio sobre la Carta de los derechos fundamentales de la Unión Europea.* Santiago de Compostela: Universidad de Santiago de Compostela.

Normativa mexicana

Ley de la Fiscalía General de la República.

Ley de la Policía Federal.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Ley Federal de Telecomunicaciones y Radiodifusión.

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

Ley General de Salud.

Ley Nacional del Registro de Detenciones.

Ley por la que se crea el banco de ADN para uso forende de la Ciudad de México.

Reglamento de la Ley General de Salud en Materia de Trasplantes.

Normativa internacional

Carta de Derechos Fundamentales de la Unión Europea.

Declaración Internacional sobre los Datos Genéticos Humanos.

Declaración Universal sobre el Genoma Humano.

Dictamen 4/2007 de 20 de junio, sobre el concepto de datos personales, del Grupo de Trabajo del Artículo 29, del Consejo de Europa.

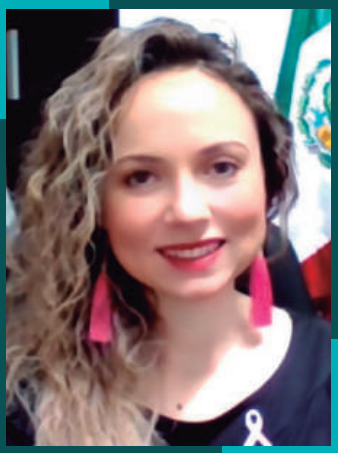
Sentencias

Sentencia del Tribunal Constitucional alemán, de fecha 15 de diciembre de 1983, en contra de la Ley del Censo. Boletín de Jurisprudencia Constitucional No. 33, 1984. p. 137-138.

Sentencia del Tribunal Constitucional de España 290/2000 de 30 de noviembre.

Sentencia del Tribunal Constitucional de España 292/2000 de 30 de noviembre.

"Datos personales biométricos
¿Qué son y cómo protegerlos?"
se terminó de imprimir en el mes de diciembre 2021
en los talleres de Smartbooks Press
La Morena 811-Loc. C Tel. 55 5697-8998 y 55 7261-7920
www.smartbooksmx.com
El tiraje consta de 750 ejemplares



Dra. María de los Ángeles Guzmán García

Doctora en Estudios Superiores de Derecho Constitucional por la Universidad Complutense de Madrid.

Máster en Diplomacia y Relaciones Internacionales por la Escuela Diplomática de Madrid.

Maestra en Derecho Constitucional y Licenciada en Derecho por la Universidad Autónoma de Nuevo León.

Profesora de la Universidad Autonóma de Nuevo León y Comisionada de la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León