UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

El Reglamento (UE) 2016/679 de la Unión Europea (Reglamento General de Protección de Datos) como referente para México en materia del derecho a la protección de datos personales en posesión de particulares.

T E S I S

QUE PARA OBTENER EL TÍTULO DE

L I C E N C I A D A E N D E R E C H O

P R E S E N T A:

PÉREZ JIMÉNEZ
ERIKA DEL CARMEN

ASESOR: MTRO. JOSÉ LUIS MANCILLA ROSALES.

Ciudad Universitaria, CD. MX., 2019

VNIVERSIDAD NACIONAL AVFNOMA DE MEXICO

FACULTAD DE DERECHO
SEMINARIO DE DERECHO ADMINISTRATIVO

Ciudad Universitaria CDMX., a 10 de Septiembre de 2019

M en C. IVONNE RAMÍREZ WENCE
DIRECTORA GENERAL DE ADMINISTRACIÓN ESCOLAR
P R E S E N T E

El pasante de esta Facultad, **PÉREZ JIMÉNEZ ERIKA DEL CARMEN** con número de cuenta **412041217** ha elaborado la tesis denominada **"EL REGLAMENTO (UE) 2016/679 DE LA UNIÓN EUROPEA (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS) COMO REFERENTE PARA MÉXICO EN MATERIA DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES"** bajo mi dirección, la cual a mi juicio cumple con los requisitos reglamentarios del caso, para ser sometido a examen profesional.

Ruego a usted ordenar lo conducente para que se continúen los trámites inherentes y dicha pasante presente el examen profesional correspondiente, en caso de no existir inconveniente para ello.

Transcribo acuerdo del Consejo de Directores de Seminarios, según circular SG/003/98, de la Secretaría General:

"La interesada deberá iniciar el trámite para su titulación dentro de seis meses siguientes (contados de día a día) a aquél en que le sea entregado el presente oficio, en el entendido de que transcurrido dicho lapso sin haberlo hecho, caducará la autorización que ahora se le concede para someter su tesis a examen profesional, misma autorización que no podrá otorgarse nuevamente sino en el caso de que el trabajo recepcional conserve su actualidad y siempre que la oportuna iniciación del trámite para la celebración del examen haya sido impedida por circunstancia grave, todo lo cual calificará la Secretaría General de la Facultad".

Reitero a usted las seguridades de mi consideración y respeto.

"POR MI RAZA HABLARÁ EL ESPÍRITU"

DRA. SONIA VENEGAS ÁLVAREZ
DIRECTORA DEL SEMINARIO
TURNO VESPERTINO

CIUDAD UNIVERSITARIA
= SEMINARIO DE DERECHO =
ADMINISTRATIVO
FACULTAD DE DERECHO

100 UNAM
UNIVERSIDAD NACIONAL DE MEXICO
1910 2010

C.c.p.- Dr.Raúl Juan Contreras Bustamante -Director de la Facultad de Derecho UNAM.
C.c.p.- Dr. Víctor Manuel Garay Garzón-Secretario General.-oficina de Exámenes Profesionales.-
C.c.p.- Alumna. Pérez Jiménez Erika del Carmen

Dedicatorías

A mi mami:

Por darme sus alas y convertirme en un alma libre, pero siempre esperar con amor que regrese a casa, por estar siempre junto a mí, a pesar de la distancia y por enseñarme a reír ante la adversidad.

Eres el mejor ejemplo de fortaleza y alegría.

Me acompañarás a donde vaya.

A mi papá:

Porque de alguna forma, desde muy niña me enseñó a no tener miedo a los cambios en la vida.

A mis hermanas:

Nata, por cuidarme y quererme siempre.

Clau, por darme tus consejos y palabras cariño.

Charo, por enseñarnos a luchar por los sueños.

Chio, por apoyarme y confiar en mí siempre a pesar de todo. Esto no sería posible sin ti.

Dani, por hacer de mi infancia un gran recuerdo.

A mis pequeñas y pequeños:

Gabi y Jorgito, Maguie y Luquita, Kele, Ale, Gabito, Dani, Diego y Chelsea, por ser la alegría de mi vida.

A mis compañeros en el camino:

Iván, por ser un confidente incondicional.

Reni, por ser la mejor amicuiii.

Eduard, por tu cariño, por enseñarme a disfrutar más de la vida y por acompañarme en esta aventura.

Y a todos los amigos que la vida puso en mi camino, Dani, Gina, Ivonne, Gabi, Leslie, Nancy, Brenda, Armando, Aarón, Marco, Cristóbal, por siempre reír conmigo.

Agradecimientos

A la vida misma, por darme una nueva oportunidad cada día, y por hacerme coincidir con seres humanos increíbles.

A mi *Alma mater,* la Universidad Nacional Autónoma de México, por darme el honor de pertenecer a la Universidad de la Nación.

A la Facultad de Derecho, por ayudar a forjar mi vida profesional y por todo lo que he aprendido de mis compañeros y maestros.

Al seminario de Derecho Administrativo, en especial a la Dra. Sonia Venegas Álvarez, por su invaluable apoyo.

A mi estimado asesor de tesis, José Luis, por el valioso tiempo que ha dedicado para apoyarme a lograr mis sueños.

Contenido

INTRODUCCIÓN

Los datos personales se han convertido en el insumo esencial para las empresas que ofrecen sus servicios en Internet. Por un lado, ellos nos ofrecen servicios “gratuitos”, y por el otro, nosotros les entreguemos nuestros datos personales como moneda de cambio.

La mayoría de estas empresas, son compañías de carácter multinacional que, gracias a la ubicuidad de Internet, pueden operar desde cualquier lugar del mundo sin necesidad de establecerse en cada país donde prestan sus servicios. Esta nueva dinámica de negocios genera que el flujo de información se extienda más allá de las fronteras nacionales.

Bajo esta tesitura, las normas en materia de protección de datos personales, deben ser adecuadas y coherentes con las necesidades de la sociedad digital y garantizar la protección de los datos aún en los flujos de información que llevan a cabo de forma cotidiana, principalmente, las grandes empresas del sector tecnológico, y que gracias a Internet trascienden el territorio de cada Estado.

Es por lo anterior, que este trabajo parte de la idea que para desarrollar un sistema jurídico adecuado en la materia se debe atender a los mejores estándares internacionales, sobre todo a los estándares europeos por ser un referente en el tema.

Tomar las mejores propuestas de otros sistemas, no solo permite tener una directriz de los países que se encuentran más avanzados en la regulación de este derecho, sino que avanza en la construcción de leyes interoperables a nivel internacional, que permitan la libre circulación de datos en beneficio de la economía digital, pero con todas las garantías para los derechos de sus titulares.

En este sentido, el propósito de esta investigación es realizar un análisis comparativo entre el nuevo estándar europeo en materia de protección de datos personales, y a partir de esto, realizar una serie de propuestas que se pueden implementar en el país, en la planeación estratégica del derecho a la protección de datos personales frente a los particulares que dominan el mundo digital.

Para ello, en esta investigación realizamos un estudio documental, y se analiza el contenido de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en comparación con el nuevo estándar europeo propuesto por el Reglamento General de Protección de Datos o RGPD de la Unión Europea (UE), por ser considerado el instrumento internacional más actualizado en la materia.

En este sentido, en primer lugar, se encuentran las consideraciones generales sobre el derecho a la protección de datos personales, su independencia respecto al derecho a la vida privada e intimidad, su reconocimiento como derecho fundamental en la UE y el nacimiento de la regulación dual que existe en nuestro país.

En un siguiente capítulo, aparecen conceptos fundamentales como “datos personales”, “datos personales sensibles” y “tratamiento”, así como el objeto y ámbito de aplicación en ambos instrumentos normativos.

A continuación, se tiene un análisis de los principios básicos más relevantes que rigen el tratamiento de datos personales, que a nuestra consideración son el principio de licitud, transparencia o información, minimización de datos y responsabilidad.

Como parte esencial, en el siguiente capítulo se estudian los derechos del interesado o titular de los datos, principalmente el derecho a la información, derecho al olvido, oposición, y derecho a no ser objeto de decisiones automatizadas, que, al mismo tiempo, se convierten en obligaciones para el responsable del tratamiento, por lo cual, también se incluyen en este apartado.

Finalmente, se incluye un capítulo dedicado a la situación actual de México en materia de protección de datos personales en posesión de particulares, a partir del análisis de las facultades del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como institución encargada de garantizar este derecho.

Para terminar, con base en el estudio comparativo, se realiza una suerte de propuesta que a nuestra consideración permitirá atender las necesidades del país en la materia.

Como esta investigación es una propuesta para desarrollar un sistema jurídico e institucional que proteja de manera adecuada el derecho a la protección de datos personales en posesión de particulares, de manera ilustrativa se hace alusión a casos emblemáticos donde estuvieron implicadas compañías como Google, Facebook y Uber, así como a tecnologías disruptivas como *big data,* almacenamiento en la nube e Inteligencia Artificial.

Estas consideraciones nos permiten mostrar de forma práctica los aciertos y desafíos que enfrenta la regulación mexicana.

En México, no se ha realizado mucha investigación desde el punto de vista jurídico, en materia de datos personales y economía de datos, lo cual dificulta comprender este derecho y su importancia en el entorno digital y tampoco es fácil encontrar información sobre las implicaciones de las tecnologías emergentes en el ejercicio del derecho a la protección de datos personales.

Por lo tanto, este estudio pretende aportar desde el Derecho, algunas ideas relevantes consideradas ya en el contexto europeo, para formular una regulación nacional en materia de datos personales que garantice este derecho en el mundo *on line.*

Finalmente, cabe aclarar que realizar un análisis comparativo no significa caer en la panacea de copiar sin saber, significa estudiarlo y adoptar aquellas directrices que sí nos ayuden a fortalecer al sistema jurídico y a las instituciones encargadas de garantizar este derecho frente a los particulares, lo que permite capitalizar los beneficios de la sociedad digital sin sacrificar aspectos tan importantes como nuestra vida privada e identidad.

CAPITULO I. CONSIDERACIONES GENERALES SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LA UNIÓN EUROPEA Y EN MÉXICO.

1. Los datos como insumo esencial de la economía digital.

El potencial del uso, aprovechamiento y explotación del espectro radioeléctrico y de las redes públicas de telecomunicaciones, así como el carácter ubicuo de Internet,[1] son elementos que han sido utilizados por diversos países para impulsar el crecimiento de la economía.

La transversalidad que los caracteriza permea en todas las actividades de la vida social, por lo que pueden ir desde dar entretenimiento y mejor acceso a servicios, hasta brindar oportunidades estratégicas para los Estados en áreas como el comercio, educación, salud, inclusión, etc., lo que permite maximizar los beneficios de la transformación digital para ganar en innovación, crecimiento y prosperidad económica.[2]

El buen funcionamiento de este nuevo modelo económico basado en Internet se debe en gran parte a la infinidad de datos que generamos en cada actividad que realizamos en línea, y que funcionan como insumo esencial para las empresas digitales, que los recogen, los procesan o tratan y lo convierten en información útil para el mejor funcionamiento de sus estrategias de negocio.

Los datos se generan desde diferentes fuentes. Cuando ingresamos a un sitio web, a una plataforma digital, compramos un producto en línea, publicamos alguna información en las redes sociales, o simplemente cuando utilizamos aplicaciones en nuestro dispositivo móvil, tableta o computadora.

Esta relación entre nosotros, nuestros datos e Internet, nos sitúa al borde de la denominada cuarta revolución industrial que, como las anteriores, está llamada a transformar buena parte, si no todos, de los ámbitos de nuestra

[1] En términos del artículo 3º de la Ley Federal de Telecomunicaciones y Radiodifusión, Internet es un "conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única."

[2] *Cfr.* Téllez Carbajal Evelyn (coord.)*, Derecho y TIC. Vertientes actuales,* t. IV: *La sociedad de la información y la equidad de género,* México, UNAM, Instituto de Investigaciones Jurídicas/INFOTEC, 2016, p. 67-73.

existencia: cómo nos comunicamos, cómo nos relacionamos, cómo producimos y cómo consumimos, en definitiva, cómo evolucionamos como sociedad. [3]

"La actual revolución está sustentada, como hemos dicho, en un elemento aparentemente más etéreo, pero, como podrá constatarse omnipresente: los datos. En la Economía del Conocimiento, los datos son insumo básico y clave".[4]

Por la importancia que han adquirido en el mundo económico, se utiliza el término Economía de datos (*Data economy* en inglés) para referirse a esta nueva forma de obtener beneficios a partir de los datos que cada empresa posee.[5]

La economía de datos, para efectos de este trabajo, es entendida como el "conjunto de iniciativas, actividades y/o proyectos cuyo modelo de negocio se basa en la exploración y explotación de las estructuras de bases de datos existentes (tradicionales y procedentes de nuevas fuentes) para identificar oportunidades de generación de productos y servicios."[6]

Este insumo esencial sobre el que se construye la economía digital tiene implicaciones directas en el derecho humano a la protección de datos personales, porque la recolección masiva de datos puede resultar, sin así considerarlo las personas, una actividad intrusiva en nuestra vida privada, al dejarnos sin la posibilidad de controlar la ubicación o finalidad nuestros datos personales, o sin la opción de controlar qué se sabe sobre nosotros y quién lo sabe.

2. El Derecho a la protección de datos personales como derecho independiente de la intimidad y vida privada.

El derecho humano a la protección de datos personales ha recorrido un largo camino antes de ser el derecho que hoy conocemos. Desde su origen, fue calificado como parte del derecho a la vida privada o a la intimidad, sin considerarse las características y objetivos particulares que lo definen en la era digital.[7]

---

[3] *Cfr.* López Sabater, Verónica y Ontiveros, Emilio, *Economía de los datos. Riqueza 4.0*, Madrid, España, Editorial Ariel, 2017, p. 11.
[4] *Idem.*
[5] *Idem.*
[6] *Ibidem,* p. 23.
[7] Cfr. Del Castillo Vázquez, Isabel Cecilia, *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar,* Pamplona, España, Editorial Arazandi, 2007, pp. 213 a 241.

En este sentido, en primer lugar es importante distinguir conceptualmente entre vida privada e intimidad, que, aunque resulta complicado pues son conceptos que están imbricados, Ernesto Garzón Valdés lo ha explicado de forma magistral:

> "Consideraré que lo íntimo es, por lo pronto, el ámbito de los pensamientos de cada cual, de la formación de decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado y que quizás nunca lo será, no sólo porque no se desea expresarlo sino porque es inexpresable."[8]
>
> "Dentro del ámbito de la intimidad caen también aquellas acciones cuya realización no requiere la intervención de terceros y tampoco los afecta: acciones autocentradas o de tipo fisiológico en las que la presencia de terceros no sólo es innecesaria sino desagradable."[9]
>
> "Es en la intimidad donde los individuos forjan su identidad, las ideas o planes de acción, que luego podrán manifestar en privado o en público, si así lo consideran, es por eso la importancia del respeto irrestricto a la intimidad y al desarrollo de ese proceso de construcción."[10]
>
> Por lo que hace a la privacidad, el mismo autor añade:
>
> "Es el ámbito reservado a un tipo de situaciones o relaciones interpersonales en donde la selección de los participantes depende de la libre decisión de cada individuo. Es un ámbito reducido, por lo que se refiere al número de sus miembros, y en él pueden darse diversas relaciones interpersonales."[11]

De esta explicación podemos deducir que la intimidad es la esencia del ser humano, lo que le queda para sí mismo frente a la sociedad, donde se está con uno mismo y la intervención de terceros no es deseada, porque es ese reducto de nuestra vista que no deseamos exponer.

---

[8] Garzón Valdés, Ernesto, "Lo íntimo, lo privado y lo público", *Cuadernos de transparencia,* México, 5ta edición, octubre de 2008, p. 15.
[9] *Idem.*
[10] *Ibidem*, p. 34.
[11] *Ibidem,* pp. 21-22.

Por lo que hace a la privacidad, es ese núcleo reducido al que pertenecemos y con el que nos permitimos compartir ciertas cosas, sin que estas deban ser reveladas a nivel público sino se desea.

Por otro lado, no obstante que el derecho fundamental a la protección de datos personales es un derecho independiente, también es un derecho ligado a los anteriores. Así nos lo plantea Troncoso Reigada:

> "La protección de datos personales, a la vez que es un derecho autónomo, es un instrumento de garantía de otros derechos fundamentales ya que la informática puede ser utilizada para limitar el pleno ejercicio de los derechos.
>
> No obstante, a nuestro juicio, el derecho fundamental a la protección de datos personales no debe ser visto como un derecho absolutamente independiente sino vinculado con el derecho a la intimidad, aunque tutele otros derechos fundamentales."[12]

En el mismo sentido, Davara Fernández de Marcos nos explica que si bien se encuentra vinculado a otros derechos, es un derecho independiente porque no se necesita una afectación a otro derecho para que este sea ejercido:

> "Es absolutamente fundamental entender que este derecho surge como consecuencia del mero tratamiento de los datos personales de un individuo, sin que se necesite, para la existencia de este derecho, que se vea lesionado ningún otro derecho. Es decir, se protege a la persona frente al tratamiento ilícito de su información personal, sin que necesitemos que se cumpla cualquier otro requerimiento de cualquier otra infracción para que pueda existir la protección."[13]

En este sentido, para fines de este trabajo, entenderemos que el derecho a la protección de datos personales es "la capacidad del ciudadano para disponer y

[12] Troncoso Reigada, Antonio, *La protección de datos personales. En busca del equilibrio*, Valencia, España, Editorial Tirant Lo Blanc, 2010, p. 1106.
[13] Davara Fernández de Marcos, Isabel, *El derecho al olvido en relación con el derecho a la protección de datos personales*, Ciudad de México, México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2014, p. 24.

decidir sobre todas las informaciones que se refieren a él,"[14] no solo las que hacen referencia a su vida privada e intimidad, sino de todos aquellos datos que le dan identidad, y que, de ponerse en riesgo, tendría afectaciones en su libre desarrollo como ser humano.

Asimismo, su protección se debe a que toda esta serie de datos que nos describen y a partir de los cuales nos relacionamos con otros, son parte de nuestra identidad, nos identifican y diferencian de los demás, y nadie, salvo las excepciones que prevea la legislación de la materia, los puede usar sin nuestra autorización, porque son garantía esencial de nuestra libertad y de nuestra dignidad humana.[15]

Por lo tanto, cada persona tiene el derecho a controlar el flujo de sus datos personales cuando interactúa con los otros, a partir de elegir qué desea comunicar, cuándo y con qué finalidad.

Para José Luis Piñar Mañas:

> "Este poder de control ha de ponerse en íntima relación con el consentimiento, que ha de ser el título esencial que justifique injerencias en nuestra privacidad.
>
> De hecho, la violación del derecho de una persona a controlar su esfera privada sea esta física o informativa, constituye el factor más importante para que se sienta invadida la privacidad. No es para ello necesario que la información sea más o menos importante o sensible.
>
> Una persona puede hacer pública información que le afecte sin que por ello considere violada su privacidad. Pero si pierde el control sobre ella, si alguien se la apropia, entonces pensará que su intimidad ha sido violada. Quien en alguna ocasión ha facilitado o ha permitido el acceso a su propia información no por ello renuncia a su privacidad."[16]

---

[14] Agencia Española de Protección de Datos, *Protección de Datos: Guía para el ciudadano*, Madrid, España, 2018. Consultado el 7 de febrero de 2019.Disponible en: *https://www.aepd.es/media/guias/guia-ciudadano.pdf*

[15] *Cfr.* López Sabater, Verónica y Ontiveros, Emilio, *op.cit.,* p. 155

[16] Piñar Mañas, José Luis, *¿Existe la privacidad?*, Madrid, España, Editorial CEU ediciones, 2008, p. 17.

Pare terminar, de lo establecido por estos autores, podemos decir, que es un derecho que arraiga en la protección a la vida privada que proviene del derecho a la intimidad, pero que no se sujeta a ellos, sino que se complementa con estos y con otros derechos más, y que su independencia radica en que no se requiere la afectación a otro derecho para ejercerlo.

Asimismo, su protección no solo es importante porque los datos nos dan identidad, sino porque su afectación puede tener implicaciones negativas en la dignidad humana.

3. La UE y el Reglamento General de Protección de Datos

La UE es quien ha marcado la pauta en materia de protección de datos personales para responder a los avances de la red (Internet) y permitir la libre circulación de los datos que necesita la economía digital, sin menoscabar el derecho de la persona sobre sus datos personales.

La normatividad europea respecto a la protección de datos personales se encuentra fundamentada en un vasto cuerpo normativo, y se considera pionera en la regulación de la materia, por lo que es observado como el mayor estándar internacional en el tema.

A lo largo de muchos años, la UE ha realizado una serie de propuestas que por su utilidad y su amplio ámbito de protección de los derechos y libertades relacionadas con la vida privada y los datos personales en el entorno digital, han sido adoptadas por los países miembros, e incluso por países que no pertenecen al espacio europeo.

Como ejemplo de este gran trabajo tenemos al Convenio 108[17], el único instrumento internacional que permite la adhesión de países no miembros de la UE, así como la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE o Carta), que se considera el primer instrumento en reconocer el derecho a la protección de datos personales como un derecho fundamental, independiente del derecho a la vida privada y familiar.[18]

---

[17] Consejo de Europa, *Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal de 1981 (Convenio 108 del Consejo de Europa),* 1981.

[18] Cfr. Troncoso Reigada Antonio*, op. cit.,* p. 175.

La CDFUE, nace en el año 2000 con la intención de crear un marco de derechos humanos aplicables en todo el territorio, y pese a estar basada en el Convenio Europeo de Derechos Humanos, la Carta resultó innovadora, en particular, por reconocer derechos fundamentales como el acceso a los documentos, la protección de datos y la buena administración.[19]

Por lo que hace a la protección de datos, desde ese momento la Carta consagró en su artículo 8:

> "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 la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
>
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente."

Este reconocimiento derivó fundamentalmente del Tribunal Europeo de Derechos Humanos que, a través de su Jurisprudencia consolidó definitivamente la diferencia entre el derecho a la privacidad y el derecho a la protección de datos personales.[20] Como resultado, a partir de este momento se le asigna una protección especial y recae sobre los Estados la obligación de garantizar su protección.

Frente a esta afirmación como derecho fundamental, la UE trabajó en actualizar la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva 95/46/CE), para adaptarla a los nuevos requerimientos de la sociedad digital.

Después de largas negociaciones en el tema por parte de las instituciones de la UE y los Estados miembros, es en 2016 que se aprueba el "Reglamento

---

[19] Cfr. Parlamento Europeo, *La protección de los derechos fundamentales en la Unión Europea,* 2019, p. 3. Consultado el 12 de marzo de 2019. Disponible en: *www.europarl.europa.eu/ftu/pdf/es/FTU_4.1.2.pdf*

[20] Cfr. Ruíz Miguel, Carlos, *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos,* Madrid, España, Editorial Civitas, 1994, pp. 49-54.

(UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de datos o RGPD).”

El RGPD, como su nombre lo indica deroga a la Directiva 95/46/CE y aunque se aprueba en 2016, entra en vigor hasta mayo de 2018 para dar oportunidad a los Estados miembros de adecuar sus sistemas al nuevo estándar.

Con esto, el RGPD se consolida como la norma más actualizada en el tema, y es de observancia obligatoria en toda la Unión, con la finalidad de evitar que la protección de datos personales sea de manera fragmentada y se otorguen diferentes niveles de protección en cada Estado miembro, como había ocurrido con la aplicación de la Directiva 95/46/CE.[21]

El nuevo estándar europeo introducido por el RGPD reconoce nuevos derechos al interesado como el derecho a la portabilidad, derecho al olvido y derecho a ser informado, e impone a los responsables del tratamiento obligaciones más firmes, como la responsabilidad proactiva junto a la rendición de cuentas y la transparencia.

El RGPD también dota de facultades y poderes amplios a las autoridades de control, al considerar que su papel es fundamental en la aplicación coherente de la normativa debido a que son las autoridades encargadas de garantizar el derecho a la protección de datos personales no solo en el territorio de la Unión, sino en todos aquellos lugares a donde viaje la información producto de la prestación de servicios de la sociedad de la información.

En este orden de ideas, el RGPD como norma vigente, es la mejor herramienta para los países fuera del espacio europeo de allegarse de conocimiento novedoso sobre el derecho a la protección de datos personales, y así, adoptar leyes que respondan a las necesidades de la sociedad digital.

[21] Considerando 9 del RGPD.

4. La dualidad de leyes en México en materia de protección de datos personales.

En nuestro país, el reconocimiento de este derecho ha seguido un camino laborioso que lo mantiene separado en un sistema de protección dual.

Por un lado, tenemos a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) del 5 de julio de 2010 aplicable al sector privado, y por el otro, a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) del 27 de enero de 2017 aplicable al sector público.

Mientras en la primera son sujetos regulados "los particulares sean personas físicas o morales de carácter privado,"[22] en la segunda "son sujetos obligados en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos"[23]

En términos generales podríamos decir que ambas leyes contemplan los mismos principios, pero al estudiarlas a fondo se vislumbra un marco jurídico más claro y robusto para el sector público, en cuestión de derechos, obligaciones y procedimientos.

Esto se debe posiblemente, a que la LGPDPPSO fue publicada en 2017, por lo cual, tuvo la oportunidad de recoger estándares internacionales más actualizados.

Previo a la publicación de esta LGPDPPSO, la protección de datos personales en posesión de organismos públicos se regía por unos cuantos artículos en la ley de transparencia. Por lo que su publicación, no solo era una instrucción constitucional, sino una demanda de la sociedad ante el vacío en la regulación aplicable al sector público.

Sin duda, es un gran logro, pero su publicación hace más evidente la regulación asimétrica que existe en el país, respecto al contenido de la LFPDPPP de 2010.

---

[22] Artículo 2º de la LFPDPPP publicada en el Diario Oficial de la Federación (DOF) el 5 de julio de 2010.
[23] Artículo 1º de la LGPDPPSO, publicada en el DOF el 26 de enero de 2017.

Esta era una gran oportunidad para el legislador mexicano de suplir las deficiencias que presenta la LFPDPPP en la era digital, o en su caso, fusionar el derecho a la protección de datos personales en un solo instrumento normativo. Contrariamente, esto no sucedió, y con ello se dejó el tema de protección de datos frente a los particulares como un derecho rezagado y de difícil aplicación.

5. El derecho a la protección de datos personales como derecho fundamental frente a los particulares.

En México, el derecho a la protección de datos personales no fue reconocido constitucionalmente sino hasta el año 2009.

La reforma constitucional de 2009, por la que se modificaron los artículos 16 y 73 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) reconoce plenamente a la protección de datos personales como un derecho fundamental.[24]

Por lo que refiere al artículo 16, se adicionó un párrafo segundo a dicho numeral, con la finalidad de establecer explícitamente el derecho a la protección de datos personales, para quedar en los siguientes términos:

> "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".

Respecto al artículo 73, en la fracción XXIX-O se dota de facultades al Congreso de la Unión "para legislar en la materia de protección de datos en posesión de particulares."

Anteriormente el Congreso ya contaba con facultades en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, pero es con esta modificación a la Constitución que se le dota con facultades sobre particulares y que se reconoce

[24] Decreto por el cual se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el DOF el 1 de junio de 2009.

explícitamente el derecho a la protección de datos personales como un derecho fundamental.

Siguiendo a Miguel Recio Gayo, "la razón para conferir al Congreso Federal la competencia en materia de protección de datos personales se debe a que, de otro modo, podrían crearse paraísos de datos personales e interponer obstáculos o barreras al comercio al interior de la República".[25]

La aplicación de la ley al sector privado "había sido ignorado debido a la renuncia a afirmar que la autoridad no solo es aquella de *iure,* sino que hay autoridades *de facto* caracterizadas en personas particulares, y que ello implica la posibilidad de que también se vulneren los Derechos Humanos en su carácter de autoridad".[26]

Para atender este nuevo mandato de la CPEUM, el 5 de junio de 2010 se publica en el DOF la LFPDPPP, y un año después, el 21 de diciembre de 2011 el Reglamento de la LFPDPPP (Reglamento).

Es así como la LFPDPPP se convierte en la encargada de regular la actuación de los particulares que realizan el tratamiento de datos personales. Frente a un mundo digital que es dominado por organizaciones o empresas privadas, este reconocimiento es fundamental para hacer del derecho a la protección de datos personales una realidad de la sociedad digital.

Como hemos dicho, la finalidad de este trabajo es comparar el nuevo estándar europeo con la legislación mexicana aplicable a los particulares, por lo cual, nos enfocamos solo en el estudio de la LFPDPPP y su Reglamento. Asimismo, consideramos que esta normativa es la que enfrenta mayores retos para su aplicación, primero, porque ha sido rebasada por la nueva LGPDPPSO aplicable al sector público y segundo, porque es la ley que deberían observar gigantes tecnológicos que recogen millones de datos en el país, como son Google, Amazon, Facebook, etc.

---

[25] Recio Gayo, Miguel, *La protección de datos en el ámbito de las telecomunicaciones e Internet,* México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2015, p. 20.

[26] Hidalgo Rioja, Ileana, *Derecho a la protección de datos personales*, México, Secretaría de Cultura, INEHRM, UNAM, Instituto de Investigaciones Jurídicas, 2018, p. 33.

6. Tecnologías disruptivas en el tratamiento de datos personales.

La recolección de datos en Internet puede resultar una actividad intrusiva en la vida privada de una persona sin que esta lo sepa, más aún, si va acompañada de tecnológicas especializadas en el tratamiento masivo de datos.

Las tecnologías disruptivas para efectos de esta investigación "son aquellas que tienen como base la innovación (*Big Data*, virtualización, *Cloud*, Ciberseguridad, Inteligencia Artificial, etc.) y tienen como denominador común su capacidad de evolucionar rápidamente y adaptarse a diferentes sectores, generando nuevos modelos de negocio."[27]

La utilización de estas técnicas o tecnologías, es una actividad asidua en las empresas actuales, sobre todo en aquellas que por su presencia mundial, manejan copiosas cantidades de información.

La utilidad de estas tecnologías en incuestionable, porque permiten realizar procesos de forma automatizada que antes no eran posibles, lo que disminuye costos en cualquier sistema productivo y aumenta las ganancias.

Sin embargo, su utilización puede traer consigo múltiples riesgos para el titular de los datos que son procesados en estas herramientas. Por un lado, porque es posible que pierda el control de sus datos y desconozca los fines para los que son utilizados, y por otro, es probable que sea objeto de evaluaciones o decisiones a partir de la elaboración de un perfil.

Estas herramientas, como veremos, permiten a quienes las utilizan, obtener información de un sinfín de datos, no necesariamente datos que se consideran datos personales, por lo cual, no se limitan en la obtención de conocimiento sobre una persona. En estas herramientas, como *big data,* cualquier dato al combinarse con otros, puede convertirse en información que identifique o haga identificable a cualquier persona.

Ante este panorama, se debe evaluar desde el mundo jurídico las implicaciones que tiene en el derecho a la protección de datos personales, el uso

[27] Sánchez del Campo, Alejandro, "Reflexiones de una replicante legal: los retos jurídicos de la robótica y las tecnologías disruptivas", *AAKAT: Revista de Tecnología y Sociedad,* Navarra, España, 2016, núm. 16, p. 153. Consultado el 12 de abril de 2019. Disponible en: *http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/383*

de estas herramientas que, por su naturaleza, permiten el procesamiento masivo de datos para la toma de decisiones, sin considerar muchas veces, los derechos de los titulares de dicha información.

CAPÍTULO II. DEFINICIONES, OBJETO Y ÁMBITO DE APLICACIÓN DE LAS LEYES EN MATERIA DE DATOS PERSONALES.

1. Importancia de conocer las definiciones, objeto y ámbito de aplicación de una ley.

"Las leyes son los instrumentos a través de los cuáles se dan los preceptos necesarios para regular la convivencia en una sociedad civilizada".[28] De ahí la necesidad de conocer su contenido, si nos encontramos en alguno de los supuestos que contempla, ya sea como responsable de cumplirla o como sujeto de derechos.

Entre los apartados que nos permiten tener una visión global del contenido de una norma se encuentran las definiciones, el objeto y el ámbito de aplicación de la misma.

Las definiciones, por un lado, nos permiten identificar de forma clara los conceptos con los que trabajamos y de esta manera llevar a cabo razonamientos de forma precisa respecto al objeto de estudio de la ley y evitar confusiones; por el otro, el objeto o ámbito de aplicación material y ámbito de aplicación subjetivo, nos indica la finalidad de la ley y las personas obligadas a su cumplimiento.

En el derecho a la protección de datos personales, el ámbito de aplicación territorial como aspecto de validez, es especialmente importante, por ser un derecho que evoluciona al paso de la sociedad *on line,* que por su naturaleza "virtual" podría tenerse como intangible desde un punto de vista físico.

Conocer y comprender el alcance de los conceptos, el objeto y la aplicación del RGPD y de la LFPDPPP nos da la posibilidad de visualizar las características particulares que adquiere este derecho cuando del entorno digital se trata y las dificultades que representa regular su ejercicio en Internet.

2. Definiciones en el RGPD

A efectos pedagógicos, porque en esta materia hay gran confusión conceptual, plantearemos estos temas en forma de "preguntas más frecuentes" (FAQ), cuyas respuestas deberían orientar la regulación que se debe seguir cuando del derecho a la protección de datos personales se trata.

[28] López Ruíz Miguel, *Redacción legislativa*, México, Senado de la República, 2002, p. 11.

2.1 ¿Qué son los datos personales?

El RGPD define a los datos personales en los términos siguientes:

"Toda información sobre una persona física identificada o identificable (el interesado).

Se considera que una persona física es identificable cuando cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un 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 de dicha persona."[29]

En términos de esta definición, los datos personales no se limitan únicamente a nombres y apellidos, sino que son una lista amplia y abierta, que va creciendo.

Los datos personales incluyen datos "como nuestra voz, número de la Seguridad Social, nuestra dirección o datos económicos. Pero también son datos de carácter personal nuestros *likes* en Facebook, nuestro ADN o nuestra forma de caminar. Ni siquiera nosotros mismos somos conscientes de las formas en las que nuestro propio día a día nos hace identificables".[30]

Asimismo, como hemos dicho, los datos personales constituyen el conjunto de referencias por el cual un individuo se define, de modo que la conjunción de todos sus datos personales configura su identidad, los cuáles al ser vertidos en Internet, configuran su identidad digital, manifestación de la primera.[31]

En las aplicaciones nativas de un dispositivo móvil, por ejemplo, se pueden recabar de modo automático datos como fotografías, videos, notas de audio, correos, contactos, etc., así como datos de localización, registros de uso de aplicaciones, consumo de datos, redes a las que se conecta el equipo, etc.

A esto hay que sumarle que el sistema operativo de algunos equipos contiene de origen, identificadores globales que podrían permitir identificar a los

[29] Artículo 4º, apartado 1 del RGPD.
[30] Gil, Elena, *op. cit.,* p. 45.
[31] Cfr. Del Castillo Vázquez, Isabel Cecilia, *op. cit.,* p. 239.

usuarios de los dispositivos, sin necesidad de que este instale una aplicación o habilite permisos en el equipo terminal. [32]

En este sentido, quien controla este tipo de aplicaciones o sistemas operativos, está en una posición privilegiada para conocer todo sobre todas las personas que utilizan un teléfono móvil.

Adicionalmente, de cara a técnicas como *big data* que veremos a continuación, que permite transformar en información útil muchos aspectos de la vida que antes no se podían cuantificar o estudiar, los datos personales deben considerarse como un conjunto de datos que no se limita a los más básicos, sino a todos aquellos datos en general que nos dan identidad, sea frente a la sociedad real o frente a la sociedad digital.

En el mismo sentido, en el Considerando 26 se especifica que "los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable".

En sentido contrario, el RGPD no es aplicable a "la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo". [33]

Elena Gil nos explica que la seudonimización "consiste en remplazar un atributo de un set de datos (normalmente un atributo único que funciona de identificador directo, como el nombre y los apellidos) por otro atributo (como, por ejemplo, el DNI, el número de Seguridad Social, o un código aleatorio que no pueda ser descifrado, de modo que no pueda conocerse a quién se refiere)". [34]

Por lo tanto, el RGPD tiene razón al considerar a los datos seudonimizados como datos personales porque todavía es posible la identificación de una persona, aun cuando se hayan cambiado unos atributos por otros, pero es cuestionable la

[32] Cfr. Agencia Española de Protección de Datos, Universidad Politécnica de Madrid, *Análisis de los flujos de información en Android. Herramientas para el cumplimiento de la responsabilidad proactiva,* Madrid, España, 2019. Consultado el 23 de marzo de 2019. Disponible en: *https://www.aepd.es/media/estudios/estudio-flujos-informacion-android.pdf*

[33] Considerando 26 del RGPD.

[34] Cfr. Gil, Elena, *Big data, privacidad y datos personales*, Madrid, España, Editor Agencia Española de Protección de Datos, 2016, p. 89.

exclusión de los datos anónimos, porque estos, aún pueden dar información sobre una persona si se combinan en técnicas como *big data.*

2.1.1 *Big data* y datos personales.

Big data o "macrodatos" en términos generales hace referencia a la "aparición y aprovechamiento de grandes volúmenes de datos (estructurados, no estructurados y semi estructurados) que, si bien algunos de ellos existían antes, nunca hasta ahora se habían contemplado como una fuente de valor para las empresas".[35]

Big data se caracteriza mediante tres *uves*: volumen, variedad y velocidad. Verónica López y Emilio Ontiveros los explican de la siguiente forma:[36]

> *Volumen***,** "es el atributo más obvio recogido en el propio término de *big data*. No en vano se ha observado una evolución desde magnitudes como los megabytes, gigabytes o terabytes hacia los petabytes".
>
> *Variedad*, "tanto en tipología de datos como sus fuentes, de forma tal que se pasa de manejar datos estructurados en bases de datos (procedentes de fuentes limitadas) y estáticos o cuasi estáticos a tratar (i) datos estructurados, semiestructurados y desestructurados; (ii) datos dinámicos o en continuo cambio, y (iii) originados por personas, máquinas, sensores, etc.
>
> *Velocidad,* **"**en la captura, el movimiento y el proceso de los datos, llegando a ser en tiempo real".

En el mismo sentido, la Comisión Europea, que es una gran impulsora de este tipo de técnicas, por los beneficios que aporta a la economía digital, define el término "macrodatos":

> "El término "macrodatos" (en inglés, *big data*) se refiere a una ingente cantidad de distintos tipos de datos procedentes de diversas fuentes, tales como personas, máquinas o sensores. Puede tratarse de datos climáticos, imágenes por satélite, fotos y vídeos digitales, registros de operaciones o señales de GPS.

[35] López Sabater, Verónica y Ontiveros, Emilio, *op. cit.,* p. 35.
[36] *Idem.*

> Los “macrodatos” pueden englobar también datos personales, es decir, cualquier información relativa a una persona y que puede ser un nombre, una foto, una dirección de correo electrónico, datos bancarios, entradas publicadas en redes sociales, información médica o la dirección IP de un equipo”.[37]

Las *uves* que caracterizan a esta herramienta desafían por excelencia las normas de protección de datos personales.

Al permitir mezclar información de diversas fuentes a gran escala, no solo datos personales en estricto sentido, sino datos de cualquier naturaleza, pueden llegar a que la identificación o re-identificación de los sujetos sea casi inminente.

Es importante recordar que el RGPD reconoce a los datos seudonimizados como datos personales, pero no a los datos hechos anónimos. En este sentido, si en los “macrodatos” se cruza información sin límites, habría que preguntarse hasta qué punto un dato puede ser anónimo.

Posiblemente el dato tratado de forma aislada no generará ninguna información sobre la persona, pero en combinación con otros, la revelación de la identidad es muy plausible. Por lo tanto, “las técnicas de anonimización no siempre son suficientes con la llegada del *big data”*.[38]

En el mismo sentido lo plantea Elena Gil, al considerar que “el análisis de grandes cantidades de datos puede llegar a identificar personas a partir de datos que nadie habría considerado de identificación personal o que antes eran anónimos, así como inferir gustos y comportamientos, a pesar de no conocer su identidad”.[39]

En este sentido, la seudoanonimización o anonimización son técnicas que no deben considerarse por sí solas como una medida que garantiza una protección efectiva, sino en combinación con otras medidas de seguridad, sobre todo, ante el crecimiento de vulneraciones a la seguridad de los sistemas en

---

[37] Comisión Europea, Dirección General de Justicia y Consumidores, *La reforma de la protección de datos en la UE y los macrodatos*. 2016. Consultado el 27 de marzo de 2019. Disponible en: *https://publications.europa.eu/es/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1*

[38] Gil Elena, *op. cit.,* p. 52.

[39] *Ibidem*, p. 88.

empresas que manejan bases de datos exorbitantes en combinan como herramientas como *big data.*

2.2 ¿En qué consiste el tratamiento de datos personales?

El artículo 4, apartado 2 del RGPD, define al tratamiento como:

> "Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

Es una definición bastante amplia, y cubre muchas actividades que se consideran tratamiento, sean estas actividades automatizadas o no.

En este sentido, aunque un tratamiento automatizado "supone una mayor amenaza para la vida privada y con ello los datos personales automatizados serán objeto de unas garantías específicas, no debemos olvidar que los datos personales no automatizados están (también) protegidos por el derecho a la vida privada".[40]

2.3 ¿Cuáles son los datos personales sensibles?

Aunque no se encuentra una definición sobre datos personales sensibles, en el Considerando 51 se establece:

> "Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales."

Asimismo, en el apartado 1 del artículo 9 se prohíbe:

> "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos

[40] Arenas Ramiro, Mónica, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, España, Editorial Tirant Lo Blanch, 2006, pp. 82-83.

biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física."

Sin embargo, en caso de ser necesario el tratamiento de estas categorías especiales, la medida será adecuada y específica a fin de proteger los derechos y libertades fundamentales de las personas.[41]

De estos artículos podemos deducir que el RGPD considera categorías especiales o datos sensibles a todos aquellos que pertenecen a la esfera más íntima de un individuo, y que su revelación tiene implicaciones determinantes en la vida del interesado, que pueden llevar a la discriminación y exclusión.

En este sentido, su tratamiento debe sujetarse a situaciones específicas, tomando en cuenta que el fin de su tratamiento no podría cumplirse de otra manera, por ejemplo si se encuentra en peligro la salud del interesado, y para ello es necesario conocer datos genéticos o su historial médico.

2.3.1 Datos biométricos como datos personales sensibles.

Los datos biométricos son conforme al inciso 14 del artículo 4 del RGPD:

"Los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos."

Troncoso Reigada nos plantea la interrogante respecto a si es compatible con la dignidad de la persona la recogida de datos del cuerpo humano, ya que esto podría significar tratar a las personas como si fueran máquinas, reduciéndolas a un algoritmo.[42]

El mismo autor continúa:

"Los datos biométricos por su propia naturaleza tratan de aportar información sobre una persona física concreta. Se eligen aquellos datos biométricos únicos -no universales- que distinguen a una persona de las demás y que generan una plantilla (o imagen) única.

[41] *Cfr.* Considerandos 51 al 57 del RGPD.
[42] *Cfr.* Troncoso Reigada Antonio, *op. cit.,* p. 217.

Si bien el algoritmo informatizado no sirve por sí mismo como elemento de identificación de personas sino se integra en un mismo fichero que incluye otros datos personales -nombre y apellidos, DNI-, sí es susceptible de identificar a las personas.

De hecho, la finalidad de los tratamientos de datos biométricos es la identificación."[43]

Bajo estas consideraciones, el tratamiento de los datos biométricos, recogidos, por ejemplo, en los sistemas de autenticación por reconocimiento facial, deben ser proporcionales con la finalidad y como hemos dicho, únicamente cuando no exista otra alternativa para atender la necesidad que motivó su tratamiento.

Si partimos de la idea de que la finalidad originaria de los datos biométricos es la identificación unívoca de una persona, al mezclarlos con otros, es altamente posible hacer a una persona identificable para siempre, debido a que el interesado no tiene la posibilidad, por lo menos accesible, de cambiarlos o modificarlos.

Así que, sin dejar de lado su gran utilidad en actividades que por su nivel de importancia requieren asegurar la identidad de una persona, su tratamiento es excepcional, y atenderá a medidas de seguridad particulares que otorguen la máxima protección, porque de verse comprometidos el interesado quedará expuesto con efectos permanentes en el tiempo.

3. Objeto y ámbito de aplicación material del RGPD

En el artículo 1 se establece que el *objeto* del RGPD es:

"1. Establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. Proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

3. La libre circulación de los datos personales en la Unión, la cual, no puede ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales."

[43] *Ibidem* p. 220.

Se advierte con esto que el RGPD es continuista de la Carta, al establecer que se protegen derechos y libertades de las personas físicas y los datos personales, no solamente la vida privada o la intimidad, sino todos aquellos que se puedan ver comprometidos en el tratamiento de los datos.

Respecto a ello, Mónica Arenas nos dice que el Tribunal Europeo de Derechos Humanos se ha pronunciado en el mismo sentido al referir que:

> "Los datos protegidos por este derecho no son únicamente los que hacen referencia a la vida privada, sino también cualquier otro dato sobre la vida pública, siempre que afecte al desarrollo de su personalidad. Porque, como es evidente, no todos los datos personales, es decir "todas las informaciones relativas a un individuo identificado o identificable" son igual de relevantes desde el punto de vista de la protección de la vida privada".[44]

La otra finalidad del RGPD es promover la libre circulación de los datos personales. Esta determinación tiene razón en términos del proyecto "Mercado Único Digital" en el que trabaja la UE.

Este proyecto busca "derribar los obstáculos entre las legislaciones nacionales pasando a un único instrumento de aplicación coherente, en favor de la libre circulación de mercancías y capitales de forma segura para lograr impulsar el sector digital como motor de crecimiento económico".[45]

"La Estrategia Europea del Mercado Único Digital tiene el propósito de mejorar el acceso de los consumidores y empresas a los bienes y servicios digitales en toda Europa, y a la creación de derechos para los productores de datos".[46]

Como es indicativo, el RGPD es parte de la estrategia de la UE de impulsar la economía digital, por lo cual, no solo se impulsa la libre circulación de datos sino que prohíbe que esta se limite por cuestiones de protección de datos personales.

---

[44] Arenas Ramiro, Mónica, *op. cit.,* p. 80.
[45] *Cfr*. Parlamento Europeo, *El mercado único digital omnipresente,* 2019. Consultado el 26 de marzo de 2019. Disponible en: *http://www.europarl.europa.eu/ftu/pdf/es/FTU_2.1.7.pdf*
[46] López Sabater, Verónica y Ontiveros, Emilio, *op.cit.,* p. 14.

En este sentido, los Estados miembros al garantizar plenamente este derecho, así como la seguridad jurídica y el mismo nivel de protección en todo el territorio, evitan crear obstáculos innecesarios al crecimiento del mercado digital.

Adicionalmente, en el artículo 2 se encuentra el ámbito de aplicación material:

> "1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
>
> 2. El presente Reglamento no se aplica al tratamiento de datos personales:
>
> a) En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;
>
> b) Por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE[47]
>
> c) Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;
>
> d) Por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

Como ya se había visto, el RGPD cubre tanto los tratamientos automatizados como los no automatizados que sean parte de un fichero o tengan esta finalidad. Un fichero es "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".[48]

Por lo cual, aun cuando los datos personales se encuentren en un soporte que no sea electrónico, pero permiten por su organización identificar a una

[47] El Título V del Tratado de la Unión Europea (TUE) contiene las Disposiciones generales relativas a la acción exterior de la Unión y disposiciones específicas relativas a la política exterior y seguridad común.
[48] Apartado 6, artículo 4º del RGPD.

persona o acceder a información sobre esta, también se encuentran sometidos a la aplicación del RGPD.

Sin embargo, como se ha dicho, el tratamiento automatizado es el que predomina, por la habilidad de cruzar información desde diversas bases de datos, estén o no estructuradas.

De las exclusiones podemos concluir que:

Primero, el RGPD solo es aplicable dentro del Derecho de la Unión, que a decir, serán la mayoría de las actividades de tratamiento de datos, debido a que la UE interfiere en casi todos los aspectos fundamentales de la economía de los países miembros; segundo, excluye a los datos personales que maneja una persona en una agenda por ejemplo, sin fines de lucro o comercialización, y tercero, se excluyen como en la mayoría de las legislaciones, el tratamiento necesario por cuestiones de seguridad pública.

4. Ámbito de aplicación territorial del RGPD.

Conforme al artículo 13 el RGPD es aplicable:

"1. Al tratamiento de datos personales en el contexto de las actividades de un establecimiento[49] del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

2. Al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago.

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. Al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros se aplique en virtud del Derecho internacional público".

[49] Según el Considerando 22 del RGPD "un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto."

En primer término, es importante celebrar la gran utilidad del RGPD al llevar su aplicación a responsables que cuentan con un estableciendo en la Unión, sin importar dónde se lleva a cabo el tratamiento, porque como veremos, la tendencia es a la aplicación del derecho del Estado donde se encuentra la información.

Actualmente, muchas son las empresas tecnológicas que ubican sus centros de datos en sus países de nacimiento o en cualquier país diferente al lugar donde ofrecen sus servicios.

Compañías como Google, por ejemplo, aunque cuentan con domicilios en diversos países, tienen la mayoría de sus servidores o *Data Center* en Estados Unidos.[50] Ante el RGPD, ya no es una excusa el lugar del tratamiento para no cumplir con la responsabilidad de garantizar la protección de los datos personales del interesado.

En segundo lugar, el RGPD es aplicable a quienes ofrecen bienes o servicios dentro de la UE, incluido quienes, elaboran perfiles derivados de un seguimiento en Internet, aunque no cuenten con un establecimiento en el territorio de la Unión.

El Considerando 23 explica que existen factores "como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión" que permiten determinar si el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

En el mismo sentido, el Considerando 24 expone que para determinar si una actividad de tratamiento controla el comportamiento de los interesados:

> "Debe evaluarse si las personas físicas son objeto de un seguimiento en Internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de

[50] Google, *Centros de Datos.* Consultado el 15 de abril de 2019. Disponible en: *https://www.google.com/intl/es-419/about/datacenters/gallery/index.html#/places*

analizar o predecir sus preferencias personales, comportamientos y actitudes".

Esta consideración parte de la idea de entender a la economía digital y sus nuevos modelos de negocio, en el que ya no es necesario que las empresas se establezcan físicamente en cada país donde ofrecen sus servicios, solo requieren insumos mínimos como acceso a Internet y una plataforma intermediaria que permita el intercambio de información entre el cliente y el proveedor.

La aparición de estos nuevos modelos de prestación de servicios por internet es una fuente de innovación que ha tenido y tiene efectos significativos en los mercados, por lo cual, la labor de los Estados es prever que su desarrollo no tenga incidencia negativa en los derechos de las personas.

En este sentido, las regulaciones en la materia deben trascender la idea cotidiana del derecho a la protección de datos personales como una cuestión doméstica, para encontrar soluciones multilaterales a problemas comunes.

4.1 *Cookies,* archivos de "seguimiento" en Internet.

La "gratuidad" de Internet se alimenta de la publicidad *on line.* A partir del análisis de los datos que dejamos en Internet, las empresas de publicidad o mercadotecnia deciden en qué categoría de consumidor se nos puede agregar y la publicidad que nos presentan conforme a nuestras costumbres de navegación.

"La sociedad aún no es plenamente consciente de la infinidad de información que revela diariamente, dejando un rastro de información que escapa a su control (por ejemplo, mediante la actividad en redes sociales, se pueden crear perfiles de usuarios según datos demográficos y, una vez procesados, pueden ser usados para generar publicidad o recomendaciones afines)".[51]

De esta manera, nuestra "huella digital", conformada por rutinas, ubicación, hábitos de consumo, páginas a las que ingresamos, etc., permiten a las empresas elaborar un retrato de cada persona sin que esta lo sepa y así, ofrecer los servicios, que, a su consideración, serán de nuestro interés. [52]

[51] López Sabater, Verónica y Ontiveros, Emilio, *op. cit.,* p. 145
[52] Cfr. Recio Gayo, Miguel, *op.cit.,* p. 65-72.

Uno de los métodos más utilizados en la generación de esta publicidad son las *cookies.*

Las *cookies,* son un "tipo de archivo o dispositivo que se descarga en el equipo terminal de un usuario con la finalidad de almacenar datos que podrán ser actualizados y recuperados por la entidad responsable de su instalación."[53]

Estas se pueden clasificar según la entidad que las gestiona, (propias o de terceros), por el plazo que permanecen activas (de sesión y persistentes) y por la finalidad de su utilización (técnicas, de personalización, de análisis, publicitarias y de publicidad comportamental).[54]

El RGPD no es ajeno a esta situación, por lo que en el Considerando 30 encontramos:

> "Las personas físicas pueden ser asociadas a identificadores en línea, facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de Internet, identificadores de sesión en forma de *cookies* u otros identificadores, como etiquetas de identificación por radiofrecuencia.
>
> Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas."

Más allá de la gran utilidad que tienen en la industria digital y en la manera más eficiente que un usuario puede consumir productos a través de la red, este "seguimiento" en línea tiene implicaciones en el derecho a la protección de datos personales, por la forma tan clara que permite crear un perfil sobre una persona.

Si bien, en cuestiones de publicidad podríamos decir que no tiene mayor problema, en otros casos podría llevar a la negación de un servicio o producto que se considera destinado a otro "tipo" de personas, y con ello promover la exclusión y discriminación.

---

[53]Agencia Española de Protección de Datos, *Guía sobre el uso de las cookies,* p.7. Consultado el 25 de abril de 2017. Disponible en: *http://www.interior.gob.es/documents/10180/13073/Guia_Cookies.pdf/7c72c988-1e55-42b5-aeee-f7c46a319903*

[54]*Ibidem,* pp. 8 y 9.

No se trata de ningún modo de prohibir su utilización, pero es necesario que al usar este u otro tipo de dispositivos o archivos de almacenamiento y recuperación de datos, los responsables informen al interesado de su existencia y la finalidad de su instalación, y que, en su caso, permitan negar el consentimiento para su utilización.

En la actualidad es de lo más común ingresar a una página web y leer frases como “utilizamos cookies para asegurar que damos la mejor experiencia al usuario en nuestro sitio web. Si continúa utilizando este sitio asumiremos que está de acuerdo”.

Este tipo de enunciados es excesivo, debido a que no se permite al usuario consentir o no, se tiene a la simple navegación en un sitio con los efectos de un consentimiento tácito.

Asimismo, es necesario que las empresas que gestionan este tipo de archivos asuman la responsabilidad de la instalación de una *cookie,* sean estas propias o de terceros, y en su caso, respondan por el tratamiento ilícito o para fines distintos de la información que recaban.

En este sentido, la aplicación fuera del espacio europeo es un gran paso que promueve la protección del derecho del interesado ante la ubicuidad de Internet y es un gran punto de partida para que los Estados se involucren en la tarea de concebir al derecho a la protección de datos personales en su dimensión internacional. De esta manera, se fomenta la cooperación entre autoridades sin invadir la esfera de actuación de cada uno en su territorio.

5. Definiciones en la LFPDPPP

Si bien en la LFPDPPP se sigue muy de cerca la línea considerada en el RGPD, vale la pena analizar también su contenido en este aspecto, porque eso nos permite visualizar de forma más clara los conceptos de los cuáles partimos y los cambios que se pueden dar en la legislación mexicana, posiblemente desde el marco conceptual.

Al igual que en el apartado anterior, lo haremos en forma de preguntas frecuentes.

5.1 ¿Qué son los datos personales?

En el mismo sentido del RGPD, la LFPDPPP define a los datos personales como "cualquier información concerniente a una persona identificada o identificable."[55]

> "Una persona es identificable cuando su identidad puede determinarse, directa o indirectamente, mediante cualquier información, y que no se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas".[56]

Los datos de tráfico o metadatos de comunicaciones, incluida la geolocalización, también se consideran datos personales, conforme a la resolución del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en 2016, por lo que, el usuario tiene derecho a acceder a ellos en caso de solicitarlo. [57]

Este reconocimiento derivó del mandado establecido en los artículos 189 y 190 de Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) que obliga a los concesionarios de telecomunicaciones y proveedores de servicios de aplicaciones y contenidos de conservar un registro de los metadatos de sus usuarios por un periodo de dos años.

En este sentido, los datos recogidos en los diferentes servicios de telecomunicaciones, ya sea telefonía fija o móvil, o en comunicaciones basadas en el protocolo IP, entran dentro del concepto de datos personales de la LFPDPPP en la medida en que identifican o permiten identificar al usuario que es persona física y titular de dichos datos.[58]

---

[55]Fracción V, artículo 3º de la LFPDPPP

[56]Fracción VIII, artículo 2º del Reglamento.

[57] En enero de 2016, un cliente de AT&T solicitó a esa compañía acceso a todos los metadatos que tuvieran sobre él, con base en la fracción II del artículo 190 de la LFTR. La compañía actuó con dilación y entregó al solicitante información que no cumplía con el derecho de acceso del titular de los datos. Por lo anterior, a petición del solicitante, se inició un procedimiento de protección de derechos. Como resultado, el INAI resolvió en junio de 2016, que los metadatos a los que se hace referencia en el artículo 190, fracción 11 de la LFTR constituyen datos personales. Consultado el 2 de abril de 2019. Disponible en:
https://sontusdatos.org/wp-content/uploads/2016/08/160713-inai-resol-xxx_c_att-ppd_0050_16-ocr-red.pdf

[58] Recio Gayo, Miguel, *op.cit.* p. 53.

Cabe precisar, que el legislador mexicano no estableció una conceptualización o parámetro de lo que debemos entender por “actividades desproporcionadas” para hacer a una persona identificable. Frente a la facilidad y rapidez con la que las actuales tecnologías permiten la identificación de una persona, no es favorable al titular de los datos personales que se dejen a interpretación estas precisiones.

Sin embargo, por la interpretación del INAI sobre los metadatos, supondremos en este trabajo, que la finalidad de una definición tan vaga es no ser demasiado descriptivo y que esto permita excluir o limitar su ámbito de aplicación. Por lo cual, deberá atenderse a cada caso en particular para saber cuándo una persona es identificable, por lo pronto, los metadatos se consideran datos que nos identifican.

5.2 ¿En qué consiste el tratamiento de datos personales?

Conforme al Artículo 3, fracción XVIII de la LFPDPPP, el tratamiento consiste en: “La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.”

Adicionalmente y de forma propositiva en el artículo 3, fracción V del mismo ordenamiento legal se establece:

> “Los datos personales podrán estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable.”

Como los hemos visto, los datos personales no solo son datos alfanuméricos, como el nombre o la CURP, sino que pueden consistir en otro tipo de información, como las fotografías en nuestro teléfono móvil o el mismo tono de nuestra voz. Por lo cual, cualquier uso que se haga de ellos, e debe considerar un actividad de tratamiento y atender a la ley aplicable.

En este sentido, mucho se ha cuestionado sobre a quién le pertenecen los datos personales que se someten a tratamiento. “Los datos son de su titular: la persona física a la que le conciernen o le afectan (en su honor, su intimidad o su

propia imagen), pero esa relación (de *suidad*) no es una relación o un derecho de "propiedad", sino un derecho personalísimo, como el derecho al honor, a la intimidad y a la propia imagen".[59]

Es decir, que los datos sean compartidos con otra persona para que esta los "trate", no significa que se cede el control sobre ellos, porque una cosa es de quien son o afectan y otra cosa diferente es quien los tiene y los trata.

En todo caso la titularidad no se pierde con el tratamiento, y en todo caso quien los tiene o trata sólo adquiere una serie de responsabilidades al obtenerlos, usarlos, divulgarlos o almacenarlos.

Los datos personales se pueden usar y hasta explotar económicamente, pero debe existir una razón clara y válida para su tratamiento, sea el consentimiento del titular o un interés legítimo.[60]

5.3 ¿Cuáles son los datos personales sensibles?

Son sensibles conforme al artículo 3, fracción VI de la LFPDPPP:

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

En términos de la definición vertida, podemos precisar que en esta se encuentran tres supuestos para considerar que los datos personales son sensibles:

En primer lugar, aquellos que refieren a la esfera más íntima de su titular. La intimidad como hemos dicho es donde los individuos forjan su identidad, por lo cual claramente son datos que de revelarse, podrían dañar la parte más esencial de la persona.

[59] López Sabater, Verónica y Ontiveros, Emilio, *op. cit.,* p. 138
[60] *Ibidem,* p. 139

En segundo lugar, aquellos datos que utilizados de forma indebida puedan causar discriminación o conlleven un alto riesgo al titular de los datos.

En términos de la fracción III del artículo 1º de la Ley Federal para Prevenir y Eliminar la Discriminación, se entiende por discriminación:

> "Toda distinción, exclusión, restricción o preferencia que, por acción u omisión, con intención o sin ella, no sea objetiva, racional ni proporcional y tenga por objeto o resultado obstaculizar, restringir, impedir, menoscabar o anular el reconocimiento, goce o ejercicio de los derechos humanos y libertades, cuando se base en uno o más de los siguientes motivos: el origen étnico o nacional, el color de piel, la cultura, el sexo, el género, la edad, las discapacidades, la condición social, económica, de salud o jurídica, la religión, la apariencia física, las características genéticas, la situación migratoria, el embarazo, la lengua, las opiniones, las preferencias sexuales, la identidad o filiación política, el estado civil, la situación familiar, las responsabilidades familiares, el idioma, los antecedentes penales o cualquier otro motivo.
>
> También se entenderá como discriminación la homofobia, misoginia, cualquier manifestación de xenofobia, segregación racial, antisemitismo, así como la discriminación racial y otras formas conexas de intolerancia."

La lista es amplia, y por lo tanto, cualquier información referida en el artículo se puede considerar como un dato personal sensible si su tratamiento menoscaba los derechos de la persona.

Debido a la complejidad de las relaciones humanas, sobre todo en la sociedad digital, este concepto es de gran utilidad para proteger a aquellos grupos o personas que históricamente han sido objeto de exclusión o segregación, y por ello, es información que merece una protección especial. [61]

En tercer lugar, aquellos datos que expresamente son reconocidos por la ley como datos sensibles, como es el caso de los datos relativos al origen racial o las preferencias sexuales.

---

[61] *Cfr.* Villanueva, Ernesto y Nucci, Hilda, *Comentarios a la Ley Federal de Protección de Datos Personales en Posesión de Particulares,* México, Editorial Liber Iuris Novum, 2012, p. 14.

En este caso, no se recogen de forma textual en la definición los datos biométricos, pero entendemos que se ubican en cualquiera de los supuestos anteriores, debido a que su utilización indebida conlleva un riesgo de identificación permanente para el titular.

Adicionalmente, conforme al artículo 9 está prohibida la creación de bases de datos sensibles, las que solo podrán crearse en casos excepcionales y siempre que la finalidad lo amerite.

Asimismo, el responsable debe obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.

Para terminar podemos decir que de acuerdo con lo delicado de la información y en relación con el grado de afectación que puede resultar para el titular de los datos, serán considerados datos sensibles o no, y de ello dependerá en gran medida, las acciones que deberá tomar el responsable para garantizar su seguridad.

6. Objeto de la LFPDPPP.

Como se desprende del artículo 1º, la LFPDPPP tiene por objeto formal “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.”

En el artículo 5º del Reglamento se aclara que dicha protección excluye a las personas morales, a la información de personas físicas con actividad comercial y a los datos de representación y contacto.

En México se constitucionalizó este derecho en el artículo 16 como el derecho a la protección de datos personales, no como el derecho a la autodeterminación informativa, por lo cual dicha diferenciación ha sido objeto de análisis por diversos autores.

Este derecho (autodeterminación informativa) junto a la privacidad, es referido como una de las finalidades de la LFPDPPP, y no se encuentra definido ni en la misma ley ni en el Reglamento, lo que da cuenta de una deficiencia de

técnica legislativa. Como es comprensible, resulta complicado proteger un derecho que no se sabe a ciencia cierta qué es.[62]

Para Osvaldo Gozaíni por ejemplo, “la autodeterminación, como lenguaje técnico tiene reminiscencias equívocas, que nos sugiere sustituirla por el “derecho a la libre disposición de datos personales”.[63]

Otros autores consideran que este derecho a la libre disposición de los datos personales supone recrear un derecho fundamental que, derivado del derecho a la vida privada del hombre, le permite resolver por sí mismo el tratamiento que quiere asignar a los datos que sobre su persona se almacenen con destinos diferentes, por lo cual, la protección de datos personales y la autodeterminación informativa pueden ser empleadas como sinónimos. [64]

Para fines de este trabajo, seguiremos a Osvaldo Gozaíni en el sentido de entender que se encuentran relacionados, pero que la autodeterminación sólo es una parte del derecho a la protección de datos personales:

> “La autodeterminación informativa constituye sólo una de las prerrogativas de la persona frente al poseedor de datos concernientes a sí mismo y la protección de datos personales en sentido amplio hace referencia al conjunto de normas jurídicas, que sistematizan, regulan y dan seguimiento al tratamiento de datos personales, son derechos que se encuentran relacionados, y que uno (autodeterminación) forma parte de la estructura más amplia del otro”.[65]

Seguimos en el mismo sentido planteado al principio de este trabajo, al considerar que la protección de datos personales es la capacidad del ciudadano para disponer y decidir sobre todas las informaciones que se refieren a él, no sólo los que refieren a la vida privada o privacidad, como refiere la LFPDPPP.

Davara Fernández de Marcos nos explica un poco más sobre la importancia de este derecho:

---

[62] *Ibidem*, p. 11.
[63]Gozaíni, Osvaldo, *Derecho procesal constitucional, habeas data, protección de datos personales*, Buenos Aires, Argentina, Editorial Rubinzal-Culzoni Editores, 2001.
[64]*Ibidem,* p. 26.
[65]*Ibidem,* p. 12 y 13.

> “La protección de datos personales cambia el paradigma, basándose ahora en la posibilidad del individuo a acceder a su información personal en posesión de cualesquiera terceros, ejerciendo este un poder de control sobre los sujetos, públicos o privados, que disponen de sus datos personales. Se pretende proteger al titular de los datos, pues corre peligro de convertirse en un ciudadano de vidrio, transparente a ojos de todos.”[66]

En el mismo sentido, Herminia Campuzano considera, que mediante el derecho a la protección de datos personales:

> “Se atribuye al titular del dato una serie de derechos como consecuencia de tal condición de propietario del dato, en aras de permitirle autotutelar su propia identidad, puesta en juego en las múltiples operaciones de registro informático que, a diversos fines, es sometida la persona durante su vida.”[67]

Esta problemática de determinar el objeto de la LFPDPPP, se hace más clara al observar que la LGPDPPSO en su artículo 1º establece que “tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados,” mientras que la LFPDPPP garantiza la privacidad y la autodeterminación informativa.

Recordemos también que la LGPDPPSO fue publicada después que la LFPDPPP, por lo que puede concluirse que, en el contexto mexicano, actualmente, se habla del derecho a la protección de datos personales en un aspecto más amplio, por lo menos, en lo que concierne al sector público.

7. Ámbito de aplicación objetivo de la LFPDPPP

En la ley no se encuentra un ámbito de aplicación objetivo, pero en el artículo 3º del Reglamento se establece:

> “El presente Reglamento será de aplicación al tratamiento de datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con

[66]Davara Fernández de Marcos, Isabel, *op.cit.,* p. 23.
[67]Campuzano Tomé, Herminia, *op.cit.,* p. 84.

independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

No se aplicarán las disposiciones del presente Reglamento cuando para acceder a los datos personales, se requieran plazos o actividades desproporcionadas."

Por su parte, las fracciones X y XI del artículo 2 del Reglamento, respectivamente definen:

Un soporte físico "es el medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales."

Un soporte electrónico "es el medio de almacenamiento al que se pueda acceder sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos personales, incluidos los microfilms."

Cabe citar a Claudia Gamboa quien nos explica:

"El derecho a la protección de datos personales, fundado en el control del individuo de la forma en que se utilizan por terceras personas, no depende del poder informático o del empleo de las nuevas tecnologías de la información y comunicaciones, estas son solo herramientas que pueden ser utilizadas para su procesamiento, pero que pueden también proveer medidas de protección adecuadas y positivas que permitan a los individuos ejercer su derecho a elegir quienes manejan, y como deben ser manejados sus datos personales."[68]

Entendemos con esto, que la LFPDPPP es aplicable por igual al tratamiento automatizado y no automatizado y sin importar si los datos se encuentran en papel o cualquier otro medio que permita acceder a ellos.

[68] Gamboa Montejano, Claudia, *Datos personales. Estudio Teórico Conceptual, de su regulación actual y de las iniciativas presentadas para la creación de una Ley en la materia (Primera Parte),* México, Cámara de Diputados LXI Legislatura, Centro de Documentación, Información y Análisis, septiembre de 2009, p. 32. Consultado el 9 de mayo de 2019. Disponible en: *http: //www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-24-09.pdf*

8. Ámbito de aplicación subjetivo de la LFPDPPP.

Como hemos visto, México cuenta con un sistema dual en materia de protección de datos personales.

Hemos tomado como punto de referencia a la LFPDPPP porque el entorno digital se caracteriza por la participación de agentes de carácter privado, y con ello, son quienes mayor control tienen sobre nuestra información. Asimismo, en la experiencia mexicana, es ante los particulares que el INAI encuentra mayores obstáculos para hacer vale la ley referida.

Por esta razón, es importancia limitar el ámbito de aplicación subjetivo, a fin de conocer cuáles son los sujetos que quedan obligados al cumplimiento de cada norma. La LFPDPPP, en su artículo 2 establece:

> "Son sujetos regulados por esta LFPDPPP, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:
>
> I. Las sociedades de información crediticia en los supuestos de la LFPDPPP para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
>
> II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial."

En el primer caso, las Sociedades de Información Crediticia regulan el tema de protección de datos en la Ley para Regular las Sociedades de Información Crediticia, donde se establece el Secreto financiero como medio para proteger los intereses del cliente.

En el segundo caso, al igual que se considera en el RGPD, estas personas carecen del ánimo de lucro en el manejo de información o datos personales, lo cual, nos lleva a pensar que el legislador buscaba delimitar claramente las personas sujetas al cumplimiento de la LFPDPPP, sobre todo en términos del crecimiento de la economía de datos.

9. Ámbito de aplicación territorial de la LFPDPPP.

La LFPDPPP tampoco determina un ámbito de aplicación territorial, pero el Reglamento precisa en su artículo 4, que el Reglamento será de aplicación obligatoria a todo tratamiento cuando:

I. Sea efectuado en un establecimiento[69] del responsable ubicado en territorio mexicano;

II. Sea efectuado por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano;

III. El responsable no esté establecido en territorio mexicano, pero le resulte aplicable la legislación mexicana, derivado de la celebración de un contrato o en términos del derecho internacional,

IV. El responsable no esté establecido en territorio mexicano y utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento. Para efectos de esta fracción, el responsable deberá proveer los medios que resulten necesarios para el efectivo cumplimiento de las obligaciones que impone la LFPDPPP, su Reglamento y demás disposiciones aplicables, derivado del tratamiento de datos personales. Para ello, podrá designar un representante o implementar el mecanismo que considere pertinente, siempre que a través del mismo se garantice que el responsable estará en posibilidades de cumplir de manera efectiva, en territorio mexicano, con las obligaciones que la normativa aplicable imponen a aquellas personas físicas o morales que tratan datos personales en México.

Cuando el responsable no se encuentre ubicado en territorio mexicano, pero el encargado lo esté, a este último le serán

[69] Conforme a la fracción IV, del artículo 4º del Reglamento, en el caso de personas físicas, el establecimiento se entenderá como “el local en donde se encuentre el principal asiento de sus negocios o el que utilicen para el desempeño de sus actividades o su casa habitación”. Tratándose de personas morales, el establecimiento se entenderá como “el local en donde se encuentre la administración principal del negocio; si se trata de personas morales residentes en el extranjero, el local en donde se encuentre la administración principal del negocio en territorio mexicano, o en su defecto el que designen, o cualquier instalación estable que permita el ejercicio efectivo o real de una actividad”.

aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III del presente Reglamento".

En México, respecto al ámbito de aplicación territorial, son diversas las problemáticas que enfrenta el INAI como garante del derecho a la protección de datos personales.

En primer lugar, porque algunas empresas multinacionales se han excusado al cumplimiento de la LFPDPPP al referir que el tratamiento de los datos se realiza en centros de datos establecidos en el territorio de otros países o que su domicilio legal los sujeta a las leyes de ese país y no al cumplimiento de la legislación mexicana.[70]

Como hemos visto, este problema también deviene de la naturaleza misma del funcionamiento de las redes y de la noción de extraterritorialidad de los datos,[71] que viene aparejado del uso de herramientas como "la nube" por diversos proveedores de servicios digitales, donde se camina hacia la deslocalización de los nuevos modelos de negocio.

Es común por ejemplo, que diversas empresas que operan en México establezcan en sus avisos de privacidad que el procesamiento de datos se lleva a cabo en otros países, y por lo tanto sujeto a otras leyes.

Por ejemplo, en la política de privacidad de compañías como Uber, se refiere que el procesamiento de datos se lleva a cabo dentro y fuera de Estados Unidos (sin especificar dónde), y que los usuarios deben considerar que, si viven en la Unión Europea o en otro lugar, el controlador de datos será: Uber B.V., ubicado en Ámsterdam.[72]

En este sentido, las facultades del INAI se ven limitadas, porque su actuación se reduce a aplicar la LFPDPPP solo en los casos en que el responsable o encargado se encuentre establecido en el país, o en su caso, se

[70]*Cfr*. IFAI, *En un hecho sin precedente, el IFAI inició un procedimiento de imposición de sanciones en contra de Google México,* México, 2015. Consultado el 29 de marzo de 2019. Disponible en: http://inicio.ifai.org.mx/Comunicados/Comunicado%20IFAI-009-15.pdf

[71] Tellez Carbajal, Evelyn (coord.), *Derecho y TIC,* t. *El Convenio de Budapest,* México, UNAM, Instituto de Investigaciones Jurídicas/INFOTEC, 2016, p. 311.

[72]Uber, *Política de Privacidad*. Consultado el 12 de mayo de 2019. Disponible en: *https://privacy.uber.com/policy*

utilicen medios situados en dicho territorio, por lo tanto, su aplicación se reduce a unos cuantos.

El ejercicio de derechos frente a estas barreras territoriales es infranqueable, y deja a la persona afectada indefensa ante las vulneraciones a sus derechos, debido a que conforme a la LFPDPPP, "consiente" el tratamiento de manera tácita al aceptar un aviso de privacidad, aunque en este se establezcan cláusulas sometidas a las leyes y jurisdicción de otros Estados.

En ese tenor, garantizar el derecho a la protección de datos personales no solo consiste en definirlo como un derecho fundamental independiente de otros, o como un derecho fundamental, sino también, en la búsqueda de construir un andamiaje jurídico innovador que se adapte a la economía digital al proteger de forma adecuada al titular de los datos sin importar dónde se encuentren sus datos.

La globalización como proceso de integración mundial en asuntos de economía, política, sociedad y tecnología,[73] aunado al flujo de información a través de redes mundiales de comunicación, generó que el derecho a la protección de datos personales sea un derecho que se desarrolla en un contexto mundial:

> "El fenómeno de su *internacionalización,* como señala PÉREZ LUÑO, radica en el reconocimiento de la subjetividad jurídica del individuo por el Derecho internacional, donde cualquier atentado contra los derechos y libertades de la persona es considerado, no ya una "cuestión doméstica" sino un problema de relevancia internacional."[74]

Este carácter de *internacionalización,* producto de la economía digital, es uno de los grandes problemas que enfrenta el derecho a la protección de datos personales. Particularmente, porque al planear la emisión de legislación en la materia se presentan cuestiones relativas a la soberanía, la privacidad y la residencia de los datos.

---

[73] *Cfr.* Flores, María Victoria, "La globalización como fenómeno político, económico y social", *Orbis,* Maracaibo, Venezuela, 2016, vol. 12, núm. 34, pp. 26-41. Consultado el 18 de marzo de 2019. Disponible en:*http://www.redalyc.org/articulo.oa?id=70946593002*

[74] Del Castillo Vázquez, Isabel Cecilia, *op. cit.,* p. 77.

Por regla general, se sigue la idea de que la información creada o almacenada de forma digital está sujeta a las leyes y regulaciones del país en que dicha información se encuentra localizada, pero como veremos ante las nuevas tecnologías como el *cloud computing,* es una apreciación que impacta de pleno en el desarrollo de la economía digital y la garantía plena del derecho a la protección de datos personales.[75]

En este sentido, la protección de datos personales es un tema que no se puede tratar de forma aislada a las regulaciones establecidas por otros países, por lo cual, una adecuada protección se puede lograr solo bajo la creación de leyes coherentes e interoperables a nivel internacional.

La coherencia e interoperabilidad de las leyes permite garantizar los mismos mecanismos y el mismo nivel de protección de un derecho en cualquier lugar o país, sin imponer demasiadas restricciones que inhiban el crecimiento de la economía digital.

Asimismo, permite superar el tema de la ubicación de los datos, al considerar que la protección no se limita a si los datos están en el territorio o no.

Caer en el error de obligar a los responsables a mantener la información en el país, o ubicar sus centros de datos en el territorio, es un retroceso en el flujo de información tan necesario para el funcionamiento de la economía y de los nuevos modelos de negocio.

Por lo cual, la cooperación entre Estados es una opción viable, así como superar el tema de la ubicación de los datos, al lograr que los responsables estén sujetos al cumplimiento de la ley con independencia de si están ubicados o no en el país.

Finalmente, es importante decir, que las instituciones garantes de este derecho en cada Estado son los puntos de conexión perfectos para generar un estado de cooperación mundial. Esta cooperación se debe hacer de forma

[75]López Sabater, Verónica y Ontiveros, Emilio, *op. cit.,* p. 155.

coordinada y armónica para evitar obstrucciones innecesarias a la libre circulación de datos personales y con ello, al desarrollo de la economía global. [76]

Asimismo, es necesario reforzar la idea de que el tratamiento de datos personales puede tener implicaciones en la dignidad de la persona, por lo cual, más allá del lugar del tratamiento se debe atender a su protección adecuada en cualquier país.

9.1 Las redes sociales

Las redes sociales son una fuente interminable de datos personales. Proporcionan un servicio gratuito que los usuarios pagan proporcionando detalles sobre sus vidas, amistades, intereses y actividades. Estos datos, su vez, son utilizados por la red para atraer a anunciantes, fabricantes de aplicaciones y otras oportunidades de negocio basadas en publicidad, principalmente.

"Como es sabido el *Bussines Model* de las redes sociales incluye el interés económico por la información personal en las mismas. Van apareciendo proyectos comerciales que se asocian a una red social o contratan sus servicios como socios terceros",[77] por lo cual, los usuarios muchas veces no saben con quién será compartida su información o el fin que se le dará.

Los mexicanos somos muy asiduos a las redes sociales. "De acuerdo con datos de la Asociación de Internet, el 90 % de la población utiliza el *smartphone.* Estas son las aplicaciones más utilizadas en México: Facebook 95%, WhatsApp 93%, Twitter 66%, Instagram 59%, Snapchat 31%, Swarm 9%"[78]

Cabe acotar, que, en México la regulación de protección de datos en las redes sociales es prácticamente inexistente, y aunque el INAI ha emitido recomendaciones útiles, como la *Guía para la configuración de privacidad en redes sociales,*[79] no existe un verdadero cuerpo normativo que haga valer los derechos frente a estas.

---

[76] *Cfr.* Palazzi A, Pablo, *La transmisión internacional de datos personales y la protección de la privacidad. Argentina, América Latina, Estados Unidos y La Unión Europea,* Ciudad Autónoma de Buenos Aires, Argentina, Editorial Adhoc, 2002, p. 95.

[77] Roig, Antoni, *Derechos fundamentales y tecnologías de la información y de las telecomunicaciones (TIC),* Barcelona, España, Editorial JMBosch, 2010, p.65.

[78] Hidalgo Rioja, Ileana, *op.cit.,* p. 50.

[79] INAI, *Guía para la configuración de privacidad en redes sociales*, México, 2018. Consultado el 9 de abril de 2019. Disponible en: *http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF*

Esta combinación de factores, por un lado, la aplicación de la LFPDPPP solo los responsables que tratan la información en el país, sumado a la falta de regulación en el tema de redes sociales, deja a los usuarios de estas expuestos ante accidentes de seguridad como el ocurrido con Facebook hace algún tiempo.

En el conocido caso de *Cambridge Analytica*, empresa de marketing político que tomó datos de usuarios de Facebook como experimento para incidir en las pasadas elecciones de Estados Unidos, más de 700 mil afectados son mexicanos, conforme a la información compartida por la misma empresa en un comunicado en sus redes sociales.

El INAI, sin posibilidad de iniciar un procedimiento, se limitó a iniciar una vía de cooperación con la empresa, debido a que Facebook, aunque cuenta con un domicilio en el país para fines de mercadotecnia, sus centros de datos están ubicados en Europa, por lo cual, la ley mexicana no le es aplicable.[80]

Por lo anterior, las personas afectadas quedaron en estado de indefensión, al no obtener por lo menos información sobre si sus datos estaban implicados, y menos aún, sin que el daño fuera reparado. En este sentido, solo queda decir que la LFPDPPP es aplicable frente a unos, pero parece ser inaplicable a los verdaderos actores en la economía de datos, como Facebook.

[80] El Financiero, *México, el quinto país más afectado por caso Facebook-Cambridge Analytica,* México, 2018. Consultado el 16 de abril de 2019. Disponible en: *https://www.elfinanciero.com.mx/tech/mexico-el-quinto-pais-mas-afectado-por-caso-facebook-cambridge-analytica*

CAPÍTULO III. PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES

Importancia de los principios generales aplicables al tratamiento de datos personales.

Los principios aplicables a la protección de datos personales cumplen una función fundamentadora, interpretativa y supletoria del ordenamiento jurídico que se trate.[81]

La Asociación Española para la Calidad determina que no sólo son meros fundamentos por los que se ha de regir la elaboración, interpretación y aplicación de la normativa sobre protección de datos, sino que se trata de un conjunto de reglas que determinan cómo recoger, tratar y ceder los datos.

En caso de encontrarnos con lagunas o vacíos legales, son una fuente de inspiración, para que el tratamiento de los datos sea conforme a la normativa. En definitiva, son deberes y obligaciones a los que están sujetos los tratamientos de datos de carácter personal.[82]

En este entendido, los principios forman junto a los derechos y obligaciones, la columna vertebral sobre la que se sostiene el derecho a la protección de datos personales.

La mayoría de los principios que enunciaremos a continuación se desarrollaron a partir de la década de los setenta, sobre todo en Europa, y han ido evolucionando conforme las necesidades tecnológicas.[83]

---

[81] *Cfr.* González Padilla, Roy, *Posesión de datos personales en posesión de particulares*, Senado de la República, Instituto Belisario Domínguez, Ciudad de México, México, 2011.
[82] *Cfr.* Asociación Española para la Calidad, *Los principios generales de la protección de datos, ¿Fundamentos y/o deberes?,* España, 2018. Consultado el 27 de mayo de 2019. Disponible en: *https://dpd.aec.es/los-principios-generales-la-proteccion-datos-fundamentos-deberes/*
[83] *Cfr.* Nava Garcés, Alberto Enrique *et.al., El derecho en la era digital. Internet, firma electrónica, protección de datos, delitos informáticos, comunicaciones, redes sociales, preservación de evidencia,* México, Editorial Porrúa, 2013, p. 59.

Aunque el nivel de reconocimiento de estos principios varía geográficamente, el RGPD recoge los principios generales más importantes y adicionalmente los inserta de una forma mejor sistematizada.

En este sentido, este apartado está dedicado a los principios que se establecen en el RGPD, y posteriormente nos ocuparemos de los principios que recoge la legislación mexicana aplicable a los particulares.

1. Principios en el RGPD.

El RGPD reconoce los principios de licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad y, responsabilidad proactiva.

Para las finalidades de este análisis, nos concentraremos en los principios de licitud, transparencia, minimización de datos y responsabilidad proactiva, porque son a nuestra consideración las áreas de oportunidad en el contexto mexicano.

1.1 Principio de licitud.

El principio de licitud como tal no se encuentra conceptualizado en el RGPD, pero en el artículo 6 del mismo establece, que el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

> “a) El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
>
> b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
>
> c) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
>
> d) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
>
> e) El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño".

El artículo básicamente se reduce a dos opciones que hacen que el tratamiento sea considerado lícito: el tratamiento basado en el consentimiento del interesado[84] o el tratamiento que se realiza sobre otra base legítima.[85]

A continuación desarrollamos cada uno:

1.1.1 El consentimiento.

La esencia de cualquier tratamiento de datos personales es el consentimiento del titular de los datos.[86]

El consentimiento del interesado ha sido siempre un concepto clave de la protección de datos, como un medio que permite respetar la autonomía de los individuos sobre la toma de sus decisiones.[87]

Se entiende al consentimiento como "toda manifestación de *voluntad libre, específica, informada e inequívoca* por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.[88]

El Grupo de Trabajo del Artículo 29 (G29)[89] desarrolló un análisis exhaustivo de la noción de consentimiento configurada en el RGPD a través de las Directrices sobre el consentimiento.[90] Para una mejor apreciación de la explicación

[84] Apartado 1, artículo 6º del RGPD.
[85] Considerando 46, 47, 48, 49 del RGPD.
[86] Cfr. Arenas Ramiro Mónica, *op. cit.,* p. 261.
[87] Gil Elena, *op. cit.,* p. 61.
[88] Apartado 11, Artículo 4º del RGPD.
[89] El Grupo de Trabajo del Artículo 29 fue creado por mandato de la Directiva 95/46/CE. Toma su nombre del artículo de la Directiva que lo crea (artículo 29). El G29 es el grupo de trabajo europeo consultivo e independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD).
[90]Grupo de Trabajo del Artículo 29, *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. Adoptadas el 28 de noviembre de 2017. Revisadas por última vez y adoptadas el 10 de abril de 2018.* Consultado el 18 de mayo de 2019. Disponible en: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051*

plasmada, se trasladan a continuación las consideraciones más importantes al respecto:

> *"Manifestación de la voluntad libre.* El término "libre" implica elección y control reales por parte de los interesados. Para que el consentimiento se considere libre debe tomar en cuenta lo siguiente:
>
> 1. Si el interesado puede realmente elegir y no existe riesgo de engaño, intimidación, coerción o consecuencias negativas importantes si no da su consentimiento.
> 2. Si el consentimiento se encuentra vinculado a la aceptación de los términos y condiciones o vinculado a la prestación de un contrato o servicio para el cual dichos datos personales no son necesarios (condicionalidad)
> 3. Si el interesado puede elegir qué fines aceptan, y cuáles no, en lugar de tener que dar su consentimiento a un conjunto de fines (disociación de los fines del tratamiento de los datos.)
> 4. Si es posible negar o retirar el consentimiento sin sufrir perjuicio alguno.
>
> *Manifestación de voluntad específica.* Debe interpretarse en línea con el requisito de «disociación» para obtener el consentimiento «libre». En suma, para cumplir con el carácter de «específico» el responsable del tratamiento debe especificar el fin como garantía contra la desviación hacia otros usos para los que no fue otorgado el consentimiento.
>
> *Manifestación de voluntad informada.* Consiste en facilitar información a los interesados antes de obtener su consentimiento para que puedan comprender qué es lo que están autorizando. Si el responsable no proporciona información accesible, el control del usuario será ilusorio y el consentimiento no constituirá una base válida para el tratamiento de los datos.
>
> *Manifestación de voluntad inequívoca.* Debe darse el consentimiento mediante una clara acción o declaración afirmativa. Una «clara acción afirmativa» significa que el interesado debe haber actuado de forma deliberada verbal (grabada), inclusive por medios electrónicos.

Puede haber incluso declaraciones escritas de muchas formas y tamaños que cumplan el RGPD. Los responsables deben evitar la ambigüedad y garantizar que la acción mediante la cual se presta el consentimiento se distinga de otras acciones.

Obtención del consentimiento explícito. El término explícito se refiere a la manera en que el interesado expresa el consentimiento. Significa que el interesado debe realizar una declaración expresa de consentimiento.

Por ejemplo, en el contexto digital o en línea, un interesado puede emitir la declaración requerida rellenando un impreso electrónico, enviando un correo electrónico, cargando un documento escaneado con su firma o utilizando una firma electrónica."

Como vemos el consentimiento implica una libre elección, que no se encuentra sometida a algún tipo de presión, es específico para cada fin, por lo cual los fines deben estar disociados de manera que se comprenda cada uno, y debe partir de la información clara y accesible que el responsable pone a disposición del interesado.

En este sentido, en el RGPD también se considera la importancia de que el interesado pueda retirar el consentimiento con la misma facilidad con la que es otorgado.[91]El consentimiento al ser una decisión reversible hace que el interesado siga manteniendo un cierto grado de control sobre su información personal.

Asimismo, establece un nivel adicional de protección en el caso de que se realice el tratamiento de los datos personales de personas físicas vulnerables, especialmente, de niños. En este caso, el artículo 8 introduce obligaciones adicionales para garantizar un mayor nivel de protección de los datos de los niños en relación con los servicios de la sociedad de la información.

El RGPD también establece que será necesario el consentimiento expreso en 3 supuestos:

1) Cuando se trata de categorías especiales de datos[92]

[91] Apartado 3, artículo 7º del RGPD.
[92] Artículo 9º del RGPD.

2) Para transferencias de datos a terceros países u organizaciones en ausencia de garantías adecuadas[93] y

3) Para la toma de decisiones individualizadas automatizadas, incluida la elaboración de perfiles.[94]

Sobre este punto, Elene Gil ahonda en el tema al abordar el problema del otorgamiento del consentimiento que se basa únicamente en el aviso de privacidad que se pone a disposición de la persona:

> "Las nuevas tecnologías tales como los dispositivos móviles, los servicios de localización, el Internet de las cosas y la existencia de sensores ubicuos, han puesto en entredicho los medios para recabar el consentimiento de los usuarios para el tratamiento de sus datos personales.
>
> La solución ha sido vista en las políticas de privacidad *online*, ofrecidas a los usuarios como términos unilaterales y (cuasi) contractuales, que se han convertido en la piedra angular de la protección de la privacidad *online*, a pesar de la aplastante evidencia de que la mayoría de las personas ni siquiera lee los términos o no los comprende."[95]

En estos términos, si bien en parte existe responsabilidad de la persona al no leer los términos establecidos en un aviso de privacidad, esto se debe fundamentalmente a que la información que se pone a disposición del interesado no es comprensible, ni clara y accesible.

En este sentido, el problema para garantizar que el consentimiento es efectivo, es decir, legítimo, atañe tanto a los usuarios como a las empresas.

Los dispositivos móviles, como hemos dicho, logran que la obtención de datos personales sea una tarea más fácil para las empresas que se benefician de estos, quienes por medio de aplicaciones que utilizamos a diario acceden a la información almacenada en el dispositivo, en ocasiones sin el consentimiento del usuario y con independencia de restricciones que el propietario establece.

---

[93] Artículo 49 del RGPD.
[94] Artículo 22 del RGPD.
[95] Gil, Elena, *op. cit.,* p. 70-71.

Cada día es más común que una aplicación requiera acceder a imágenes, ubicación, contactos, etc., sin que el usuario comprenda la relación que tiene el fin de la aplicación con el acceso a este tipo de datos.

Peor aún, muchas de ellas, funcionan y acceden a todo tipo de datos sin la necesidad de obtener la autorización o permisos por parte del usuario, y sin que este tenga conocimiento de ello.

Un estudio difundido por la Agencia Española de Protección de Datos y realizado este año por el Instituto IMDEA Networks y la Universidad Carlos III de Madrid acerca del software preinstalado en dispositivos Android, que abarcó más de 82.000 *apps* preinstaladas en más de 1.700 dispositivos, revela la existencia de un complejo sistema de desarrolladores y acuerdos comerciales en el que las *apps* preinstaladas disponen de permisos privilegiados, sin que el usuario lo sepa o tenga la posibilidad de desinstalarlas.[96]

Aparte de los permisos estándar definidos en Android y bajo control del usuario, los investigadores identificaron más de cuatro mil permisos propietarios o personalizados por los intervinientes en la fabricación de los terminales.

"Este tipo de permisos permite que aplicaciones publicadas en Google Play eludan el modelo de permisos de Android para acceder a datos del usuario sin requerir su consentimiento al instalar una nueva *app."*[97]

Finalmente, como hemos dicho, la obtención de un consentimiento legítimo es uno de los problemas a los que se enfrenta el derecho a la protección de datos personales, y un punto clave en el cumplimiento del principio de responsabilidad proactiva, por el cual, el responsable al saber que la nueva tecnología a implementar llevará a cabo el tratamiento de datos personales, debe considerar la privacidad desde las primeras fases de diseño de esta nueva tecnología, sea una aplicación, equipo, o sistema operativo en el caso de la telefonía móvil.

Al respecto, Eduardo Riestra dice:

---

[96]Instituto IMDEA Networks, Universidad Carlos III de Madrid, *An Analysis of Pre-installed Android Software*, Madrid, España, 2019. Consultado el 15 de mayo de 2019. Disponible en: *https://haystack.mobi/papers/preinstalledAndroidSW_preprint.pdf*

[97]*Idem.*

"Otorgar el consentimiento informado debería ser fácil, tanto en el acceso como en su comprensión. En este sentido, el consentimiento se encuentra intrínsecamente ligado al derecho a que se le proporcione información clara y al derecho de acceder a la información.

En el caso de la toma de decisiones automatizadas, se requiere el consentimiento expreso, lo que permite, que el interesado tome una decisión consciente de otorgar o no la autorización para el tratamiento. Pero en gran medida su consentimiento dependerá de lo comprensible de la información."[98]

Es a través de la adopción de medidas adecuadas que se puede proteger la información del usuario desde el diseño de un proyecto, con lo que se previene en gran medida, la vulneración de los derechos del interesado.

Asimismo, la actuación de los responsables o fabricantes de equipos móviles, sistemas operativos o aplicaciones deben actuar conforme a los principios en materia de protección de datos personales, en este caso, principalmente sobre el principio de lealtad y transparencia.

1.1.2 Bases legítimas para el tratamiento de datos diferentes al consentimiento

El RGPD también prevé que el tratamiento puede basarse en bases jurídicas distintas al consentimiento. Para que dicha base funja como una base legítima para el tratamiento debe ser clara y precisa y su aplicación previsible para sus destinatarios. Por lo tanto, requiere una evaluación meticulosa, y que constituya una medida necesaria y proporcional en una sociedad democrática.[99]

Conforme al artículo 6, apartado 1, las bases legítimas distintas al consentimiento para llevar a cabo el tratamiento pueden ser:

"1) La ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales,

2) El cumplimiento de una obligación legal aplicable al responsable del tratamiento,

[98] *Cfr.* Riestra Herrera, Eduardo, *Privacidad en el Diseño de la Inteligencia Artificial*, España, Asociación de Marketing de España, España, 2017, pp. 9-14.
[99] *Cfr.* Considerando 41 del RGPD.

3) Para proteger intereses vitales del interesado o de otra persona física,

4) Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento) y

5) Para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales".

Si bien el tratamiento puede estar formulado sobre una de estas bases, y el consentimiento pasa a un segundo plano, es una obligación del responsable informar al interesado que se lleva a cabo dicho tratamiento.

Igualmente, es el responsable quien deberá demostrar que es viable realizar el tratamiento sobre una base jurídica distinta al consentimiento.

Con esta consideración de alternativas al consentimiento, el nuevo RGPD pone al mismo nivel de este las otras bases legítimas para el tratamiento. A estas alturas, todavía no sabemos hasta dónde llegará la interpretación del "interés legítimo" de una empresa para poder tratar los datos de una persona sin su consentimiento, aspecto clave para la explotación y la Economía de los Datos.[100]

1.2 Principio de lealtad y transparencia

"Del principio de lealtad se desprende la obligación del responsable de adoptar una actitud honesta y abierta en relación con los datos que trata, de manera que, dicho responsable solo trataría datos de forma que no puedan generar un efecto negativo o injustificado respecto de los titulares de los datos".[101]

El principio de transparencia obliga al responsable del tratamiento a establecer toda una serie de medidas que garanticen un correcto entendimiento por parte del interesado de todo lo relativo al tratamiento de sus datos personales.[102]

---

[100] López Sabater, Verónica y Ontiveros, Emilio, *op. cit.,* p. 140.

[101] *Cfr.* Lorenzo Cabrera Sara *et.al., Protección de datos, responsabilidad activa y técnicas de garantía. Curso de "delegado de protección de datos" adaptado a la nueva LFPDPPP orgánica 3/2018 de 5 de diciembre de protección de datos personales y garantía de los derechos digitales,* Madrid, España, Editorial Reus, 2018, p. 43.

[102] *Idem.*

Conforme al RGPD este principio exige que el responsable ponga a disposición del interesado cierta información que le permita conocer la manera en que se lleva a cabo el tratamiento de sus datos personales.

La información que entregue debe ser gratuita, concisa, transparente, entendible y accesible, y que se utilice un lenguaje sencillo y claro. En particular, debe poner especial atención en cualquier información dirigida específicamente a un niño, que por su condición merecen una protección específica. [103]

La información debe ser entregada al interesado en el momento que se obtengan de ellos los datos personales para el tratamiento[104] o, si se obtienen de otra fuente, en un plazo razonable,[105] dependiendo de las circunstancias del caso.[106]

La información que se ponga a disposición del interesado debe cuando menos contener la identidad del responsable del tratamiento, los fines del mismo la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento.[107]

1.2.1 Características de la información

En las Directrices sobre la transparencia en virtud del RGPD 2016/679[108] emitidas por el G29, se esclarece las características de la información que se debe poner a disposición del interesado:

Concisa y transparente. Implica que los responsables del tratamiento deben presentar la información o comunicación de manera eficiente y sucinta para evitar la fatiga informativa. Esta información debe diferenciarse claramente

[103] *Cfr.* Considerando 58 del RGPD.
[104] Artículo 13 del RGPD.
[105] Artículo 14 del RGPD.
[106] Considerando 61 del RGPD.
[107] Considerando 39 del RGPD.
[108] Grupo de Trabajo del Artículo 29, *Directrices sobre la transparencia en virtud del RGPD 2016/679. Adoptadas el 29 de noviembre de 2017. Revisadas por última vez y adoptadas el 11 de abril de 2018.* Consultado el 8 de mayo de 2019. Disponible en: *https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/wp260rev01_es-transparencia.pdf*

de otra información no relacionada con la privacidad, como las disposiciones contractuales o las condiciones generales de uso.

Inteligible. Debe resultar comprensible al integrante medio de la audiencia objetivo. La inteligibilidad está estrechamente vinculada al requisito de utilizar un lenguaje claro y sencillo. Un responsable del tratamiento que actúe con responsabilidad proactiva conocerá a las personas sobre las que recopila información y puede utilizar este conocimiento para determinar lo que dicha audiencia es susceptible de comprender.

De fácil acceso. El interesado no debe tener que buscar la información, sino que debe poder reconocer inmediatamente dónde y cómo acceder a esta información. En el caso de las aplicaciones, la información necesaria también debe estar disponible en la tienda en línea antes de la descarga. Una vez instalada la aplicación, es preciso que la información siga siendo de fácil acceso desde dentro de la aplicación. Una manera de cumplir este requisito es garantizar que, para llegar a la información, no hagan falta más de «dos toques» (p. ej., incluyendo una opción de «Privacidad» / «Protección de datos» en la función de menú de la aplicación).

Lenguaje claro y sencillo. La información debe facilitarse de la forma más simple posible, evitando oraciones y estructuras lingüísticas complejas. La información debe ser concreta y categórica; no debe formularse en términos abstractos o ambivalentes ni dejar margen para distintas interpretaciones. Para ello, debe evitarse el uso de calificativos del tipo «puede», «podría», «algunos», «frecuentemente» y «posible». La información facilitada a un interesado no debe contener lenguaje o terminología de naturaleza excesivamente legal, técnica o especializada.

Bajo las consideraciones vertidas, la información debe presentarse al interesado de manera eficiente y sucinta y que sea información comprensiva al usuario promedio, por lo cual, el lenguaje utilizado deber ser claro y sencillo, y permitir que se acceda a esta información de manera fácil, sin tener que buscarla de manera laboriosa.

El principio de transparencia es un principio que refleja el principio de lealtad y de responsabilidad proactiva, que busca que el responsable lleve a cabo el tratamiento sin opacidad, con lo cual, se genera confianza en los procesos que afectan al ciudadano ofreciéndole información útil que lo capacite para entenderlos.

Por lo anterior, este principio es fundamental en la obtención del consentimiento libre e informado. Si la persona no obtiene información que revele de forma clara la finalidad de un tratamiento, el consentimiento carece de validez.

Por ser uno de los principios más importantes en el tratamiento de datos, ha sido motivo de la primera multa impuesta en términos del RGPD.

En diversas notas periodísticas se informaba a principios de este año, 2019, que Google era multada en Francia con 50 millones de euros por "falta de transparencia, información incorrecta y ausencia de consentimiento válido en la publicidad personalizada".

Conforme a estas la Comisión Nacional de Informática y Libertades (CNIL), el organismo francés encargado de velar por la protección de datos determinó que “la información no era fácilmente accesible, a veces era necesario hacer hasta cinco clics para acceder a esta información”.[109]

Esta resolución es de gran importancia al establecer que no es suficiente que un responsable informe al interesado el uso que se hará de sus datos, sino que es necesario que dicha información sea realmente clara y accesible.

Como establecía Elena Gil, el consentimiento se ha dejado a los avisos o declaraciones de privacidad que nadie lee. Peor aún, al no ser accesibles, si existiera algún usuario interesado en conocerlo, desistirá sin duda de esa labor al darse cuenta que existe una cierta imposibilidad de comprender su alcance y contenido.

[109] Como ejemplo la nota publicada en el periódico La Vanguardia el 21 de enero de 2019. Consultada el 17 de junio de 2019. Disponible en: *https://www.lavanguardia.com/tecnologia/20190121/454234917044/francia-multa-google-50-millones-infringir-proteccion-datos.html* y la nota publicada en El país el mismo día. Disponible en: *https://elpais.com/economia/2019/01/21/actualidad/1548088756_370588.html*

Por lo cual, cumplir o no con el principio de transparencia antes de recoger la información del interesado, es un punto de partida que determinará la licitud o ilicitud de un tratamiento.

1.3 Principio de minimización de datos

En términos del artículo 5º apartado 1, inciso c) del RGPD, los datos personales deben ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)"

Para cumplir con el principio de minimización, por lo tanto, el responsable no puede requerir al interesado más datos personales de los necesarios, a la vez que la persona interesada no está obligada a dar más datos de los estrictamente necesarios para que se cumpla la finalidad establecida.

En este sentido, los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios.[110]

Para Troncoso Reigada, este principio consigue frenar el conocimiento excesivo que pueden llegar a obtener terceros sobre una persona física. Así, la información sometida a tratamiento estará directamente vinculada a la finalidad a la que se destina tal recopilación.[111]

Como en el caso anterior, existen aplicaciones que precisan de ciertos permisos para prestar el servicio, como *WhatsApp* que acceda a los contactos registrados en el directorio de un teléfono celular. En este caso, se puede considerar que el permiso solicitado es necesario para cumplir la función de la aplicación.

Por el contrario, existen muchas aplicaciones que solicitan por ejemplo acceder al almacenamiento del equipo en general, lo cual es contrario al principio de minimización, o por ejemplo, una aplicación cuya finalidad es la práctica de un idioma, no tendría por qué obtener datos de la galería de fotos, las conexiones de red, o cualquier otro dato que no tenga relación con su finalidad.

Big data, en este punto, parece ser todo lo contrario a lo que establece el principio de minimización. Como hemos visto, una de sus virtudes es estudiar

[110] *Cfr.* Considerando 39 del RGPD.
[111] *Cfr*. Troncoso Reigada, Antonio, *op. cit.*

cantidades masivas de datos (volumen) lo que le permite obtener conocimiento para la toma de decisiones. [112]

Cabría la posibilidad de pensar que el principio de minimización, aunque es deseable, no es necesariamente aplicable a estas técnicas, siempre y cuando se cumpla con el resto de los principios y se garantice de manera fehaciente los derechos del interesado.

En último término, más allá de la importancia de reducir el número de datos que se recogen, se debería atender a cuál es el uso que se les dará, "en esto radica la *data science,* como conjunto de técnicas que permiten pasar de un almacén de datos a las aplicaciones de valor con los mismos".[113]

En otras palabras, dependerá más del destino que se le dé a la información obtenida, por ejemplo, si son utilizados para la creación de nuevos productos y servicios o para elaborar un perfil discriminatorio, que al número de datos proporcionados por la persona. Esto, solo es aplicable en determinados casos.

En lo general, los datos que se someten a tratamiento deberán ser los indispensables para el cumplimiento de la finalidad.

1.4 Principio de responsabilidad proactiva.

Definir a la responsabilidad proactiva como un principio es una de las novedades que ofrece el RGPD. Este principio consiste en la obligación del responsable de llevar a cabo las acciones necesarias para cumplir los principios del tratamiento de datos, y a su vez, ser capaz de demostrarlo (rendición de cuentas).[114]

"El principio de *accountability* o rendición de cuentas se manifiesta como una apuesta clara para promover una actitud más proactiva del responsable a la hora de demostrar que, no solo cumple con las exigencias en materia de protección de datos, sino que, además debe disponer de elementos que demuestren tal cumplimiento. Se pasa por tanto de un enfoque reactivo a uno proactivo".[115]

---

[112] *Cfr.* Riestra Herrera, Eduardo, *op.cit.,* p. 57.
[113] López Sabater, Verónica y Ontiveros, Emilio, *op. cit*., p. 43.
[114] Artículo 5º, apartado 2 del RGPD.
[115] Lorenzo Cabrera, Sara *et.al*., *op.cit.* p. 47-48.

La responsabilidad proactiva se verá reflejada en las medidas de seguridad tomadas por las empresas en el tratamiento de datos, como la privacidad desde el diseño y por defecto, las evaluaciones de impacto, entre otras, que analizaremos en el apartado de obligaciones.

2. Principios en la LFPDPPP

Los principios reconocidos en la LFPDPPP se articulan y actualizan en cada ocasión donde el particular proporcione a un tercero sus datos.

Dicha entrega y manejo, deberá ajustarse a los principios referidos, para permitir al titular de los datos ejercer el poder de control que tiene sobre la información personal que le concierne, sobre su utilización y destino, para evitar utilizaciones ilícitas.[116]

Los principios recogidos en la LFPDPPP son el principio de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.[117] A continuación, se enumeran los más importantes, para conocer su contenido y alcance.

2.1 Principio de licitud

Conforme al artículo 7 de la LFPDPPP:

> "Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta ley y demás normatividad aplicable.
>
> La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.
>
> En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta LFPDPPP."

En el Reglamento, artículo 44 se explica que existe actuación fraudulenta o engañosa cuando:

---

[116] *Cfr*. Tenorio Cueto, Guillermo Antonio *et.al., Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares,* México, Editorial Porrúa, 2010, p. 56

[117] Artículo 6º de la LFPDPPP.

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

II. Se vulnere la expectativa razonable de privacidad del titular

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

En estos términos, Nava Garcés nos dice, que el principio de licitud obliga entonces al responsable a que "el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional, y con pleno cumplimiento de la legalidad y respeto de la buena fe y los derechos del individuo".[118]

En el mismo sentido, la Doctora Vanessa Díaz lo explica de la siguiente manera:[119]

"El principio de licitud se refiere a la forma de recolección y tratamiento de la información personal, la cual deberá ser obtenida y procesada de forma justa y de acuerdo a la LFPDPPP de la materia.

El segundo párrafo del artículo establece la interpretación de este principio, el cual se base en determinar si los datos personales se obtuvieron de manera justa, así como en el cuidado del método de obtención.

El último párrafo de este artículo se refiere a la buena fe; en la mayoría de las legislaciones y documentos internacionales se considera un principio fundamental".

Respecto al deber de confidencialidad, la misma autora considera:

"El legislador mexicano utiliza el término privacidad en el contexto de razonable privacidad. Sin embargo, consideramos que el legislador no debió utilizar dicho término, ya que, en estricto sentido, en el tratamiento de los datos personales no puede existir una "expectativa razonable de privacidad" existe la expectativa razonable de confidencialidad, que se genera a través de las relaciones personales, sociales, financieras, culturales entre los mismos individuos e instituciones privadas".

[118] Artículo 10 del Reglamento.
[119] Nava Garcés, Alberto Enrique *et,al*., *op. cit.,* p. 67.

En este sentido, veremos en su momento, que el deber de confidencialidad es una de las obligaciones más importantes del responsable y encargado, quienes, derivado de la confianza que el titular de los datos ha depositado en ellos al compartirles su información, deben guardar “secreto” respecto a esta y no compartirla con terceros no autorizados.

2.2 Principio de consentimiento

Conforme al artículo 8, se reconoce al consentimiento como un principio en el tratamiento de datos personales, y que obliga al responsable a obtenerlo del titular de los datos para el tratamiento, a menos que no sea exigible conforme a las excepciones previstas en la LFPDPPP.

La solicitud del consentimiento deberá ir referida a una finalidad o finalidades determinadas, que se encontrarán previstas en el aviso de privacidad.

En términos del artículo 3, fracción IV de la LFPDPPP y artículo 11 del Reglamento, debe entenderse al consentimiento como “el poder de decisión y control que goza el titular de los datos sobre el tratamiento de estos, y que es principal fuente de legitimación del tratamiento de los datos personales por parte del sujeto regulado.”

Dicho consentimiento debe darse de forma previa, libre, específica, informada e inequívoca[120] y será según la naturaleza de los datos personales expreso o tácito.[121]

El titular podrá negar o revocar su consentimiento, así como oponerse para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular, sin que ello tenga como consecuencia la conclusión del tratamiento para estas últimas finalidades.[122]

Para ello, el responsable deberá establecer mecanismos sencillos y gratuitos, que permitan al titular revocar su consentimiento al menos por el mismo medio por el que lo otorgó, siempre y cuando no lo impida una disposición legal.[123]

[120]Artículo 12 del Reglamento.
[121] Artículo 8º y 9º de la LFPDPPP.
[122] Artículo 8 de la LFPDPPP y artículo 21 del Reglamento.
[123] Artículo 21 del Reglamento.

Ante la negativa por parte del responsable de cesar el tratamiento de los datos derivado de la solicitud de revocación del consentimiento por parte del titular de los datos, el titular podrá presentar ante el INAI la denuncia correspondiente para iniciar un procedimiento de verificación.[124]

Salvo que la LFPDPPP exija el consentimiento expreso del titular, será válido el consentimiento tácito como regla general,[125] y se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.[126]

Cabe referir en este apartado que considerar que se ha entregado un consentimiento válido por el solo hecho de poner a disposición del titular de los datos el aviso de privacidad, parece una apreciación excesiva por parte del legislador.

Considerar el silencio del titular al no objetar el aviso de privacidad, como un consentimiento tácito, sin tomar en cuenta si el aviso de privacidad cumple con todos los requisitos conforme al principio de información, tiene efectos negativos en los derechos del titular de los datos.

En primer lugar, porque como hemos dicho, los avisos de privacidad que el responsable pone a disposición del usuario en la mayoría de los casos no son ni claros y mucho menos se encuentran separadas las diferentes finalidades para las cuales se recoge cada dato, por lo cual, el titular no tiene la opción de otorgar un consentimiento informado, específico e inequívoco u oponerse al tratamiento para determinados fines.

Segundo, porque el consentimiento real debería ser libre. “Sin embargo, en la práctica, vivimos en un contexto de “lo tomas o lo dejas”. Esta circunstancia no debería ser tan preocupante si se sancionaran las conductas abusivas”.[127]

Pongamos, por ejemplo, el caso de algunas de las aplicaciones de transporte privado que utilizamos frecuentemente. (Uber, Cabify, DiDi).

---

[124] Artículo 22 del Reglamento.
[125] Artículo 13 del Reglamento.
[126] Artículo 8º de la LFPDPPP.
[127] López Sabater, Verónica y Ontiveros, Emilio, *op. cit.,* p. 152.

Cuando descargamos la aplicación para acceder al servicio, no existe la posibilidad para el usuario de manifestar su “oposición” a determinadas cláusulas que contiene el aviso de privacidad, y que resultan confusas, inentendibles o innecesarias para el cumplimiento de la finalidad.

El usuario que desea o tiene la necesidad de utilizar el servicio, debe aceptar la totalidad del contenido del aviso de privacidad, debido a que no existe la posibilidad de oponerse en el primer contacto a determinados usos de nuestra información que hará el responsable.

Es decir, si el usuario usa un servicio en el que ha aceptado el aviso de privacidad, no significa que esté totalmente de acuerdo con el contenido de este o que otorgue su consentimiento pleno, significa que no cuenta con alternativas para negarse o aceptarlo de forma parcial en caso de que no esté de acuerdo con determinados fines.

Entonces, “pareciera ser que no es tan conveniente un consentimiento tácito, menos aun cuando la ley lo reconoce como un requisito o supuesto que no es excepcional”[128]

En este sentido, la valoración de la validez del consentimiento no se desprende de la simple y llana puesta a disposición de un aviso de privacidad, sino de considerar si este cumple con las características de la información, y las condiciones con base en las que se considerará que se puso a disposición del titular, pues así podría tenerse mucha mayor certeza de que no se vulnera el principio de información y consentimiento.[129]

2.2.1 Excepciones a la obtención del consentimiento.

Conforme al artículo 10 de la LFPDPPP, no es necesario el consentimiento para el tratamiento de los datos personales cuando:

“I. Esté previsto en una ley

II. Los datos figuren en fuentes de acceso público;

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

[128] Hidalgo Rioja, Ileana, *op.cit.,* p. 34.
[129] *Cfr.* Tenorio Cueto, Guillermo Antonio *et.al*., *op. cit.,* p. 59.

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

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

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

VII. Se dicte resolución de autoridad competente".

Las excepciones al consentimiento del titular de los datos, podríamos decir que se asemejan a las bases legítimas distintas al consentimiento, consideradas en el RGPD.

Todas parecen ser situaciones que requieren una intervención inmediata, en las que esperar a obtener el consentimiento podría tener un perjuicio mayor, (por ejemplo, en el caso de atención médica al titular de los datos); o de situaciones que responden a un mandato de ley o de la autoridad.

Sin embargo, llama la atención, aquella excepción que hace referencia a los datos personales que son sometidos a un proceso previo de disociación.

De acuerdo con la LFPDPPP, la disociación es el "procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo."[130]

Cabe señalar que la LFPDPPP no señala las técnicas como el cifrado o la anonimización, que se pueden considerar para alcanzar un grado de "disociación" adecuado en ciertos casos, para determinar que el consentimiento no es necesario.

Como hemos referido las tecnologías emergentes como *big data* que acceden y cruzan información de diversas bases de datos logran la identificación o

[130] Fracción VIII del artículo 3º de la LFPDPPP.

re-identificación de una persona de forma casi innata, por lo cual, es necesario determinar que no todas las técnicas pueden lograr que los datos dejen de ser asociados a una persona.[131]

A nivel doctrinal se ha llegado a la conclusión que, dependiendo del tipo de datos, también dependerá el nivel de disociación.[132] Sería de gran importancia en este punto, que el INAI como experto en la materia estableciera parámetros mínimos para considerar en qué grado un proceso técnico como el cifrado, anonimización o seudonimización son factibles de considerar y cuál es el grado de disociación que se ofrece en cada uno.

Igualmente, en caso de no ser el consentimiento el fundamento para tratar los datos, existen otras causales igualmente legítimas para llevarlo a cabo, pero estas deberán ser acreditas en su momento, por el responsable del tratamiento.

El dilema sobre el consentimiento como se refirió en páginas anteriores deriva de la problemática para determinar si la información que se ha dado al titular de los datos es comprensible o no, en términos de su situación particular. El consentimiento tal y como está previsto en la actualidad no soluciona los problemas prácticos que presenta este y el siguiente principio.

Por lo cual, tal vez el modelo de consentimiento informado ya no deba ser la piedra angular del tratamiento de datos.[133]

Más que hablar sobre el consentimiento del titular, como base que legitima el tratamiento por excelencia, es necesario observar si la información que conoce el titular le permite conocer en realidad los alcances de este y, por otro lado, apostar por promover el cumplimiento del principio de responsabilidad y la rendición de cuentas, en el que, uno de los puntos clave es el uso responsable que se le da a la información obtenida.

“En un nuevo sistema, el requisito del consentimiento debería reservarse para usos relevantes, de forma que los individuos presten una atención mayor

[131] Cfr. Riestra Herrera, Eduardo, *op.cit.,* pp. 47-50.
[132] Cfr. Nava Garcés, Alberto Enrique *et.al., op. cit.,* p. 88.
[133] Cfr. Gil, Elena, *op. cit., p.* 122.

cuando el consentimiento les es requerido, y de este modo sea un mecanismo más efectivo".[134]

2.3 Principio de información (deber de notificación)

Conforme al artículo 15 de la LFPDPPP y 23 del Reglamento, el principio de información consiste en la obligación del responsable de informar a los titulares sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, con objeto de que pueda ejercer sus derechos a la autodeterminación informativa, privacidad y protección de datos personales.

El medio idóneo para hacerlo conforme a la LFPDPPP es el aviso de privacidad.

2.3.1 Aviso de privacidad

El principio de información se materializa en la puesta a disposición del aviso de privacidad en cualquiera de sus tres modalidades: integral, simplificado y corto,[135] a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.[136]

El aviso de privacidad es el "documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales,"[137] por el cual el responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines.[138]"

Si los datos se obtienen personalmente del titular, el responsable deberá poner a su disposición el aviso de privacidad integral; si se obtienen de manera directa o indirecta del titular, el responsable podrá poner a su disposición el aviso de privacidad integral o el simplificado, y cuando el espacio utilizado para la obtención de los datos personales sea mínimo y limitado, se podrá utilizar la modalidad de aviso de privacidad corto.

En términos del artículo 24 del Reglamento de la LFPDPPP, a fin de que el aviso de privacidad sea un mecanismo de información eficiente y práctico, este

---

[134] *Ibidem,* p. 134.
[135] Cfr. Lineamientos del Aviso de Privacidad, publicado en el DOF el 17 de enero de 2013.
[136] Artículo 17 de la LFPDPPP.
[137] Fracción I del artículo 3º, de la LFPDPPP.
[138] Artículo 15 de la LFPDPPP.

será “sencillo, con información necesaria, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento”.

Para ello, deberá:

“I. No usar frases inexactas, ambiguas o vagas; como “entre otros datos personales o por ejemplo".

II. Tomar en cuenta para su redacción los perfiles de los titulares;

III. No incluir textos o formatos que induzcan al titular a elegir una opción en específico;

IV. En caso de que se incluyan casillas para que el titular otorgue su consentimiento, no se deberán marcar previamente, y

V. No remitir a textos o documentos que no estén disponibles para el titular”.

Asimismo, el aviso de privacidad integral deberá contener, al menos, la siguiente información:[139]

“I. La identidad y domicilio del responsable que trata los datos personales

II. Los datos personales que serán sometidos a tratamiento.

III. El señalamiento expreso de los datos personales sensibles que se tratarán;

IV. Las finalidades del tratamiento, lo cual se logra de conformidad con el artículo 40, segundo párrafo del Reglamento de la Ley, cuando con claridad, sin lugar a confusión y de manera objetiva se especifica para qué objeto serán tratados los datos personales;

V. Los mecanismos para que el titular pueda manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que no son necesarias, ni hayan dado origen a la relación jurídica con el responsable;

VI. Las transferencias de datos personales que, en su caso, se efectúen; el tercero receptor de los datos personales, y las finalidades de las mismas;

VII. La cláusula que indique si el titular acepta o no la transferencia, cuando así se requiera;

VIII. Los medios y el procedimiento para ejercer los derechos ARCO;

[139] Artículo 16 de la LFPDPPP y artículo 26 y 27 del Reglamento.

IX. Los mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento al tratamiento de sus datos personales;

X. Las opciones y medios que el responsable ofrece al titular para limitar el uso o divulgación de los datos personales;

XI. La información sobre el uso de cookies, web *beacons* u otras tecnologías similares y sobre el hecho de que a través de las mismas se obtienen datos personales, así como la forma en que se podrán deshabilitar, esto último salvo que dichas tecnologías sean necesarias por motivos técnicos.

XII. Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad".

Los avisos de privacidad, si bien se consideran un gran avance en el derecho mexicano al recoger en un extracto el principio de información, no han logrado su finalidad como garantía del derecho a la protección de datos personales, porque siguen siendo para el usuario un texto interminable, poco claro y engorroso que no se lee.

En el caso del aviso de privacidad simplificado o corto, estos no contienen la información suficiente para que el titular de los datos conozca la naturaleza del tratamiento, por lo tanto, la reducción de información parece no ser la solución.

Como hemos dicho, el mero hecho de poner a disposición del titular el aviso de privacidad, no significa que el consentimiento sea otorgado de manera inequívoca, clara y específica. Mucho menos informada. "Una política de privacidad ideal ofrecería a los usuarios verdadera libertad de elección, sobre la base de una comprensión suficiente de lo que implica dicha elección".[140]

Aunque la LFPDPPP contempla que el titular de los datos puede oponerse al tratamiento de sus datos para ciertas finalidades, que no derivan de la relación jurídica entre este y el responsable, este punto no es respetado entre los responsables del tratamiento. Pocas veces se informa que existe dicha posibilidad.

Es decir, que no basta que se informe al interesado el uso de *cookies, web beacons* u otras tecnologías similares de seguimiento en Internet, sino que debe

[140] Gil, Elena, *op. cit.,* p. 71.

existir la posibilidad real de negarse u oponerse a su uso, y a las consecuencias que deriven de ellas, sean la creación de perfiles, decisiones individuales automatizadas o cualquier otra.

En este sentido, algunos autores opinan que los deberes de información y la necesidad de recabar el consentimiento debe referirse, no solo al hecho de que se recaben datos primarios, sino también a la información que se puede extraer de un análisis sofisticado de éstos, incluyendo la información que pueda extraerse de la agregación de datos que recaba la empresa con datos provenientes de otras fuentes y ficheros.[141]

Así, por ejemplo, el titular de los datos debería conocer tanto los datos recabados como los motivos en que se basa una decisión automatizada o la inclusión en determinado perfil.

No obstante, esta aproximación tiene dificultades prácticas en técnicas como *big data* que, por su propia naturaleza, el valor que genera reside precisamente en lo inesperado de los resultados que revela, por lo cual, la utilidad del aviso de privacidad es nula, porque no se puede informar algo que no se sabe.[142]

Adicionalmente, como ha quedado establecido, la ubicuidad de Internet permite la prestación de servicios a través de la red, sin que una empresa se establezca físicamente en cada país, por lo cual, muchos avisos de privacidad son desarrollados de forma genérica, de acuerdo con los requerimientos establecidos por las leyes del país de origen del particular, no necesariamente basados en la legislación mexicana.

En este sentido, la protección o garantías aplicables que este aviso de privacidad pudiera contener tampoco podrán ser reclamadas por el titular en caso de vulneración de sus derechos, al constituirse un problema jurídico de aplicación por la “territorialidad” del derecho exigible, sumado a la complejidad que tendrá para una persona iniciar un procedimiento contra una compañía fuera del país.

[141] *Ibidem,* p. 73.
[142] Cfr. Riestra Herrera, Eduardo, *op.cit.,* pp. 57-58.

Los usuarios se encontrarán entonces obligados a respetar los términos establecidos, por plataformas internacionales como Facebook, pero no son sujetos de derechos respecto a la misma.

En estos términos, el aviso de privacidad no es una garantía plena de información, por lo cual, México se convierte en un "paraíso cibernético", principalmente, para aquellas empresas a las que no se les puede obligar al cumplimiento de la LFPDPPP.

2.3.2 Notificación de una vulneración de seguridad.

En el mismo sentido, la LFPDPPP considera que como parte del principio de transparencia, se encuentran las notificaciones de vulneraciones de seguridad al titular de los datos.

Por lo cual, el responsable tiene la obligación de informar de forma inmediata al titular de los datos las vulneraciones de seguridad que afecten de forma significativa sus derechos patrimoniales o morales, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.[143]

Al respecto, la LFPDPPP no determina cuándo una vulneración de seguridad se constituye en una afectación significativa para los derechos del titular, con lo cual, se deja a discreción del responsable informar o no al titular afectado.

Tampoco está previsto, que se notifique al INAI, lo cual, deja en total determinación del responsable la forma de actuación respecto a los datos personales que se encuentren implicados en un accidente de seguridad. Ante el desconocimiento, el ejercicio de derechos es inexistente.

2.4 Principio de responsabilidad

En términos de los artículos 6 y 14 de la LFPDPPP el responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por dicho ordenamiento legal, debiendo adoptar las medidas necesarias para su aplicación.

Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable, por lo que el responsable deberá tomar las medidas

[143] Artículo 20 de la LFPDPPP.

necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.

Como nos dice Tenorio Cueto:

> "Este principio ordena a todo tratante a no adoptar medidas menores a las que adoptaría tratándose del manejo de su información. El tratante se obliga a prever medidas contra cualquier riesgo, las consecuencias emanadas de la vulneración de cara a los titulares y, sobre todo, actualizar su desarrollo tecnológico de cara a posibles vulneraciones de seguridad".[144]

Este principio funciona como garantía para el titular de los datos personales, quien deposita su confianza en el sujeto obligado, de que este los conservará y tratará con la diligencia medida, para lo cual, implementará medidas tendientes a su protección y conservación.

Es una relación que funciona en principio bajo la buena fe, en que se piensa que el responsable actuará conforme a la ley, y para asegurar el tratamiento legítimo solo por parte de los autorizados adopta medidas de seguridad adecuadas antes y durante el tratamiento.

Para cumplir con este principio el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.[145]

2.4.1 Esquemas de autorregulación vinculante

Los esquemas de autorregulación vinculante en materia de protección de datos personales tienen como objeto *complementar* lo dispuesto por la LFPDPPP, el Reglamento y cualquier otra disposición aplicable en la materia, así como demostrar ante el Instituto y los titulares el cumplimiento de obligaciones previstas en dicha normativa.[146]

---

[144] Tenorio Cueto, Guillermo Antonio *et.al*., *op. cit,* p. 58.
[145] Artículo 47 del Reglamento.
[146] Artículo 44 de la LFPDPPP y artículo 79 del Reglamento.

“Contendrán reglas o estándares específicos que permitan armonizar los tratamientos de los datos personales efectuados por los adheridos y facilitar el ejercicio de derechos por parte de los titulares”.[147]

Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos. [148]

Conforme al artículo 48 del Reglamento, entre las medidas de autorregulación que se pueden tomar, se encuentran:

> “La elaboración de políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable, programas de capacitación y concientización, sistemas de supervisión y vigilancia interna para comprobar el cumplimiento de las políticas de privacidad, procedimientos para mitigar riesgos cuando implemente nuevos productos, servicios o tecnologías, revisión periódica de las políticas y programas de seguridad, y procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales”.

Asimismo, se deberán considerar sanciones por el incumplimiento de estas medidas y contar con un conjunto de acciones técnicas y administrativas que permitan garantizar el cumplimiento de los principios y obligaciones.

Al tener en cuenta la vulnerabilidad de los sistemas de seguridad, como se ha dicho, estas medidas deben funcionar en cooperación unas con otras, porque la mera aplicación de una sola no garantizará para nada la correcta actuación del responsable, y con ello, tampoco la seguridad de la información.

Además, hay que tener presente que son medidas complementarias a la LFPDPPP, es decir, que no basta con implementarlas, sino que deben garantizar el debido tratamiento, privilegiando los intereses del titular y la protección de sus datos personales, así como su concordancia con la ley.

---

[147] Nava Garcés, Alberto Enrique *et.al., op cit.,* p. 137.
[148] Artículo 80 del Reglamento.

En el caso de los códigos de conducta o códigos deontológicos, es una medida que “no parece ser tan efectiva como se predica,[149] por lo cual, debe ser parte de un sistema de seguridad más robusto y no entenderse de manera aislada como medida suficiente.

Se debería en este caso, promover que el INAI participe en la elaboración de estos mecanismos, para garantizar que contengan un nivel adecuado de protección.

La Organización para la Cooperación y el Desarrollo Económico (OCDE) ha planteado que el concepto de responsabilidad aún no ha logrado una amplia aceptación en la región latinoamericana, por lo cual, es necesario trabajar más en su implementación:

> “México es el único país que lo incluye en su legislación y regulación nacionales sobre protección de datos. Sin embargo, el grado en que los responsables del tratamiento de datos aplican este principio no está completamente claro. Además, la mayoría de las leyes de protección de datos de los países LAC no obligan a implementar un programa de gestión de la privacidad”.[150]

Bajo esta tesitura, si bien el principio está contemplado en la ley es necesario fortalecerlo y aclarar ciertas cuestiones como su aplicación en todo el proceso de tratamiento. De esta manera, la responsabilidad que ahora parece recaer en el titular de los datos, se comparte de alguna manera con el responsable del tratamiento, quien finalmente, será el que obtiene los beneficios económicos.

[149]Palazzi A. Pablo, *op. cit.,* p. 70

[150]Cfr. OCDE/BID, *Políticas de banda ancha para América Latina y el Caribe: un manual para la economía digital,* OECD, Paris, 2016. Consultado el 10 de mayo de 2019. Disponible en: *http://dx.doi.org/10.1787/9789264259027-es*

CAPÍTULO IV. DERECHOS Y OBLIGACIONES RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES

La Organización de las Naciones Unidas ha afirmado en diversas ocasiones, que los mismos derechos que tienen las personas fuera de línea también deben protegerse en línea, por lo que los Estados deben hacer frente a los problemas de seguridad en Internet de conformidad con sus obligaciones internacionales de derechos humanos para garantizar la protección *on line* de los derechos humanos.

A nivel internacional se ha reconocido que algunos derechos humanos por su naturaleza se ven mayormente afectados por la inmersión en el entorno digital. Tal es el caso del derecho a la protección de datos personales.

Tanto el RGPD como la LFPDPPP reconocen un conjunto de facultades al interesado o titular de los datos derivado del derecho a la protección de datos personales, como instrumento propio para controlar la actuación del responsable ante el tratamiento de sus datos personales, sobre todo por el uso de herramientas que permiten el tratamiento automatizado a gran escala.

Estos derechos se encuentran interrelacionados y van ampliando su interpretación, ante los requerimientos de la sociedad de la información.

En el caso de México aún falta mucho para reconocer o dotar de contenido derechos que ya se recogen en estándares internacionales, particularmente en el contexto europeo, como el derecho de portabilidad, derecho al olvido y el derecho a oponerse a decisiones individuales automatizadas.

Los derechos que veremos a continuación son oponibles frente a los responsables, y por lo tanto una obligación.

1. Derechos del interesado en el RGPD.

En el caso del RGPD, se reconoce al interesado los derechos de información, acceso, rectificación, supresión y derecho al olvido, limitación del tratamiento, portabilidad, oposición y decisiones individualizadas automatizadas.

En este trabajo, abordaremos únicamente el derecho de información, supresión y derecho al olvido, portabilidad y derecho de oposición y decisiones

individuales automatizadas, porque son los derechos que aún no han sido desarrollados en México.

1.1 Derecho de información.

Como hemos visto, el principio de transparencia exige que el responsable ponga a disposición del interesado cierta información que le permita conocer la manera en que se lleva a cabo el tratamiento de sus datos personales.

Conforme al artículo 12 esta debe ser gratuita, concisa, transparente, entendible y accesible, y que se utilice un lenguaje sencillo y claro, en particular cualquier información dirigida específicamente a un niño, que por su condición merecen una protección específica.[151]

El RGPD aborda de forma tangencial el tema del tratamiento de los datos de niños y niñas. Por ello, “el deber de informar adquiere caracteres especiales en el caso de los menores.

En efecto, al tratarse de personas en desarrollo, la información que se dirija a ellos debe estar adaptada a sus capacidades de entendimiento. Sólo así se puede garantizar el cumplimiento de este deber y que el menor presta el consentimiento habiendo comprendido la información relativa al tratamiento de sus datos personales, es decir, siendo consciente de para qué lo presta”.[152]

En un derecho fundamental en el ejercicio de los derechos restantes, por lo que se podrá ejercer por el interesado en tres momentos que veremos a continuación:

1.1.1 Conocer información relacionada con el tratamiento.

Es el derecho del interesado a obtener toda la información relacionada con el tratamiento de los datos, en el momento que estos se obtienen, o si se obtienen de otra fuente en un plazo razonable, dependiendo de las circunstancias del caso, la cual se pondrá a su disposición mediante el aviso de privacidad, política de privacidad o declaración.

---

[151] Considerando 58 del RGPD.

[152] Andreu Martínez, Ma. Belén, *La protección de datos personales de menores de edad*, Navarra, España, Aranzandi SA, 2013, p. 137.

En el Artículo 13 se enuncia la información que deberá facilitarse al interesado cuando los datos personales se obtengan de este directamente, principalmente la identidad y los datos de contacto del responsable, los datos de contacto del delegado de protección de datos, los fines del tratamiento y los destinatarios o las categorías de destinatarios de los datos personales.

También se le debe informar si se llevan a cabo transferencias a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación, o referencia a las garantías adecuadas o apropiadas, los derechos del interesado, la existencia del derecho a retirar el consentimiento en cualquier momento y el derecho a presentar una reclamación ante una autoridad de control.

En el inciso k) del mismo artículo se establece que debe informarse al interesado la existencia de decisiones automatizas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias de dicho tratamiento para el interesado.

Si los datos no se obtienen directamente del interesado, el RGPD prevé que se le informe adicionalmente sobre las categorías de datos personales de que se trate y la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.[153]

Es importante en este caso, que se inscriba dentro de la información que debe conocer el interesado, la elaboración de perfiles y la existencia de decisiones basadas únicamente en un tratamiento automatizado de datos, debido a que muchas veces es información que se desconoce, lo que podría generar un uso abusivo de los datos al clasificar a las personas en categorías o perfiles discriminatorios que reproduzcan estereotipos y exclusión.

En caso de no estar informado, no podría ejercer el derecho a que se rectifiquen los datos o que se anulen, en caso de una decisión basada únicamente en el tratamiento automatizado, y que, por un error, y ante el desconocimiento sea víctima de discriminación. [154]

[153] Artículo 14 del RGPD.
[154] Cfr. Riestra Herrera, Eduardo, *op.cit.,* p. 65-66.

En este particular, la entrega de información deberá ser especialmente clara para el interesado y requiere de un esfuerzo extra por parte del responsable, a fin de transformar información técnicamente compleja que deriva de algoritmos matemáticos, en datos fácilmente digeribles para un usuario normal. Sobre esto, hablaremos más adelante.

1.1.2 Solicitar información en cualquier momento.

En términos del mismo artículo 12, es el derecho a formular una solicitud de información al responsable en cualquier momento posterior a la recogida, para conocer sus actuaciones respecto del tratamiento de los datos personales.

La solicitud de información se convierte a su vez en la obligación del responsable de disponer todos los medios para facilitar al interesado información sobre sus derechos y sobre cómo ejercerlos.

En estos casos, el responsable solo podrá negarse a actuar frente a una solicitud de derechos si puede demostrar que no está en condiciones de identificar al interesado,[155] o cuando la solicitud sea manifiestamente infundada o excesiva, especialmente debido a su carácter repetitivo.[156]

Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

Es un derecho que básicamente consiste en que el responsable cree los mecanismos adecuados para que el interesado ejerza sus derechos cuando lo considere necesario.

1.1.3 Notificación de las violaciones de seguridad

Es el derecho del interesado a que se le comunique sin dilación las violaciones de seguridad a sus datos personales, que entrañen un alto riesgo a los derechos y libertades de las personas físicas.

[155] Apartado 2 del artículo 12 del RGPD.
[156] Apartado 5, inciso b) del artículo 12 del RGPD.

Esta comunicación debe realizarse tan pronto como sea razonablemente posible y en cooperación con la autoridad de control competente, para que el afectado pueda tomar medidas a fin de mitigar un mayor daño en sus derechos.[157]

En las Directrices sobre notificación de vulneraciones de seguridad que emitió el G29 se explica la naturaleza de esta notificación. Lo concerniente, lo abordaremos en el apartado de obligaciones.

En general, podemos decir que el derecho de información es un derecho con implicaciones en todo el tratamiento de datos personales, y forma parte esencial del principio de lealtad y responsabilidad proactiva, y busca transparentar los procedimientos por los cuales el responsable realiza el tratamiento

Si este no se materializa previo a la obtención de los datos, se vulnera tanto la capacidad de decidir del interesado si está de acuerdo o no con el tratamiento de sus datos personales, el ejercicio de otros derechos y, posteriormente, la decisión de retirar el consentimiento en caso de conductas contrarias al RGPD.

No informar al interesado, por ejemplo, la ocurrencia de una violación de seguridad, lo deja en estado de indefensión ante el desconocimiento del riesgo en el que se encuentran sus derechos y libertades fundamentales. Por lo cual, es una de las obligaciones más importantes que debe cumplir el responsable en cuando sus sistemas de seguridad han sido vulnerados.

1.2 Derecho de supresión

El artículo 17, apartado 1, hace referencia al derecho de supresión, anotando entre paréntesis el derecho al olvido, como si estos fueran uno mismo. Sin embargo, a lo largo del texto los separa y más aún, determina que el derecho al olvido es un derecho posterior o que deriva del derecho de supresión.

En el mismo artículo, se inscribe que el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan cuando estos:

- Ya no sean necesarios en relación con los fines para los que fueron recogidos

[157] Artículo 34 del RGPD.

- Se ha basado en el consentimiento prestado al responsable y se decide retirarlo, siempre que el citado tratamiento no se base en otra causa que lo legitime.
- El interesado ha ejercido su derecho de oposición, y no prevalecen otros motivos para legitimar el tratamiento,
- Los datos personales hayan sido tratados ilícitamente,
- Deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento,
- Se hayan obtenido en relación con la oferta de servicios de la sociedad de la información,[158] a menores de edad.

Cuando el responsable haya hecho públicos los datos personales y esté obligado, a suprimir dichos datos, "teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos".[159]

Es en este último párrafo donde el derecho al olvido comienza a formar su contenido.

1.3 Derecho al olvido

Se conoce como derecho al olvido, a un interés jurídicamente protegido de los ciudadanos que consiste en lograr efectivamente que sus datos personales no sean localizados por los buscadores en la Red.[160]

Andreu Martínez nos explica que este derecho es especialmente importante cuando se trata de menores:

---

[158] En la Directiva 98/48/CE del Parlamento Europeo y del Consejo de 20 de julio de 1998, se establece que un servicio de la sociedad de la información es "todo servicio prestado normalmente a cambio de una remuneración, a distancia (un servicio prestado sin que las partes estén presentes simultáneamente), por vía electrónica (un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite) y a petición individual de un destinatario de servicio (un servicio prestado mediante transmisión de datos a petición individual)".

[159] Apartado 2, artículo 17 del RGPD.

[160] Álvarez Cano María, Derecho al olvido en Internet. *El nuevo paradigma de la privacidad en la era digital,* España, Editorial Reus, 2015, p. 71.

> “Tratándose de los menores, la previsión específica en relación con este derecho respecto de los datos proporcionados cuando el interesado era un niño pretende proteger a la persona frente a actuaciones realizadas cuando todavía no tenía la capacidad de obrar (y podía no ser consciente de los riesgos asumidos), evitando además la creación de perfiles desde edades tempranas”.[161]

El RGPD es un poco general al abordar el tema, pero en el Considerando 66 establece que:

> “A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos”.

En la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE), encontramos uno de los casos más publicitados respecto a este derecho y el papel de los motores de búsqueda como Google.

Esta controversia suscitada en 2014 entre la Agencia Española de Protección de Datos Personales (AEPD) y Google Spain,[162] bajo la interpretación de la Directiva 95/46, abrogada por el RGPD, el TJUE determinó que Google, también era responsable del tratamiento de los datos, debido a que “recoge tales datos que extrae, registra y organiza posteriormente en el marco de sus programas de indexación, conserva en sus servidores y, en su caso, comunica y facilita el acceso a sus usuarios en forma de listas de resultados de sus búsquedas”.

En este sentido, si se ejerce el ejercicio del derecho al olvido, y es procedente, tiene la obligación de retirar enlaces cuando se realiza una búsqueda por el nombre del interesado.

[161] Andreu Martínez, Ma. Belén, *op. cit.,* p. 149.
[162] *Cfr*. Álvarez Caro, María, *op. cit.,* pp. 90-110

Más recientemente, en una disputa nuevamente entre Google, la Comisión Nacional de Tecnologías de la Información y Libertades Civiles (CNIL) de Francia y varias organizaciones británicas e internacionales de libertad de expresión iniciada en 2017, se abordó el mismo tema.

En esta ocasión, para determinar si la obligación de los motores de búsqueda como responsables del tratamiento es aplicable a nivel mundial o solo en la información que sea accesible desde la Unión Europea.

Al respecto, el Abogado General del TJUE emitió una opinión considerando que el gestor de un motor de búsqueda está obligado a suprimir los enlaces controvertidos solo cuando la búsqueda sea realizada desde un lugar situado en la Unión Europea.

El responsable entonces solo está obligado a tomar las medidas a su alcance para garantizar una retirada de enlaces eficaz y completa, en particular, la técnica del "bloqueo geográfico" desde una dirección IP supuestamente localizada en uno de los Estados miembros.[163]

Cabe acotar que la interpretación que ha realizado el abogado general es también conforme a la Directiva 95/46, por resultar la LFPDPPP aplicable al momento en que se inició el procedimiento,[164] por lo cual, será necesario esperar para conocer el posicionamiento final del Tribunal en términos del RGPD.

En este sentido, se necesita mucha más jurisprudencia al respecto, que permita ir dotando de contenido al derecho y determinar cuál es su campo de actuación ante el Internet mundial y ubicuo.

---

[163]Szpunar, Maciej, Abogado General, Tribunal de Justicia de la Unión Europea, *CONCLUSIONES DEL ABOGADO GENERAL SR. MACIEJ SZPUNAR presentadas el 10 de enero de 2019 (1), Asunto C‑507/17, Google LLC, que se ha subrogado en los derechos de Google Inc. contra Commissionnationale de l'informatique et des libertés (CNIL), con intervención de Wikimedia Foundation Inc., Fondationpour la liberté de la presse, Microsoft Corp., ReportersCommitteeforFreedomof the Press y otros, Article 19 y otros, Internet FreedomFoundation y otros, Défenseur des droits,* enero 2019. Consultado el 26 de marzo de 2019. Disponible en:
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62017CC0507&qid=1565060402063&from=EN

[164]*Ibidem*, apartado 32.

Muchos son los ciudadanos europeos que han acudido a diversos prestadores de servicios en la red, principalmente motores de búsqueda y redes sociales, para ejercer su derecho al olvido.

Se debe considerar también que el ejercicio del derecho al olvido en muchos casos está motivado por la desconfianza de la población en las empresas que recogen nuestros datos personales, por lo cual, más que impulsar el ejercicio de este derecho, se debe buscar un aumento de la seguridad jurídica y del refuerzo de la confianza en el entorno digital.

Con esto se fomentará un círculo virtuoso entre la protección de un derecho fundamental, la confianza de los consumidores y el crecimiento económico.

El RGPD determina que, por regla general, el derecho al olvido se verá limitado "cuando el tratamiento sea necesario para ejercer el derecho a la libertad de expresión, para el cumplimiento de una obligación legal del responsable, por razones de interés público en temas de salud pública, de archivo, fines de investigación científica o histórica y para la formulación de reclamaciones".[165]

Ahora, si son aplicables las conclusiones del Abogado General del TJUE, también se encontrará limitado a las IP que se encuentren en la UE.

Para terminar, podemos decir que a la hora de configurar un derecho al olvido digital es de vital importancia el establecimiento de límites y excepciones para hacerlo viable y además respetuoso con otros derechos fundamentales de las personas y con los intereses de todos los agentes implicados.

"En el caso de introducir un derecho al olvido digital sin límites ni excepciones se estaría creando una presunción de que la privacidad está por encima de otros valores como la libertad de expresión, información, el periodismo, la investigación, la literatura, la seguridad nacional, entre otros".[166]

[165] Apartado 3, artículo 17 del RGPD.
[166] Álvarez Cano, María, *op.cit.,* p. 80.

1.4 Derecho de oposición y derecho a no ser objeto de decisiones individualizadas automatizadas

La redacción de este precepto puede resultar un poco confusa, al ver que el legislador europeo incluyó en un solo apartado ambas opciones. Debido a lo anterior, a primera vista se podría considerar como un único derecho (oposición).

Sin embargo, es a partir de las siguientes consideraciones que podemos interpretar el contenido del derecho de oposición y del derecho a no ser objeto de decisiones individuales automatizadas.

Respecto al primero, el RGPD reconoce en el artículo 21 que el interesado tiene derecho a oponerse al tratamiento de sus datos personales, en términos de su situación particular, bajo alguno de estos siguientes supuestos:

- El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento
- El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable o de un tercero, siempre que no prevalezcan sobre estos los derechos del interesado.
- Es un tratamiento con fines de mercadotecnia directa (incluida la elaboración de perfiles). Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.
- Al tratamiento con fines de investigación científica o histórica o fines estadísticos, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Respecto al derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles, el RGPD establece en su artículo 22:

> “1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado.

3.En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4.Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado".

Este derecho tiene estrecha relación con el derecho a ser informado, y por ello en el artículo13, inciso f) y 14, inciso h), se establece que se debe informar al interesado cuando se recaban sus datos:

"La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado."

Conforme al RGPD los responsables pueden llevar a cabo la elaboración de perfiles y adoptar decisiones automatizadas siempre que cumplan todos los principios y dispongan de unas bases jurídicas para el tratamiento.

En el caso de decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, se aplican garantías y

restricciones adicionales, como la necesidad de intervención humana en la toma de decisiones.

Para explicar esto, el G29 emitió las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 (Directrices sobre decisiones automatizadas).[167]

Las Directrices separan la elaboración de perfiles y las decisiones automatizadas, indicando que no necesariamente suceden al mismo tiempo, sin embargo, es posible que la elaboración de un perfil termine en una decisión automatizada, o viceversa. Por lo cual, se debe atender al tipo de tratamiento para conocer sus efectos en la vida de las personas.

La explicación contenida en las Directrices es muy entendible y permite comprender conceptos que podrían resultar complejos por sus tecnicismos.

En los apartados siguientes se anotan las consideraciones más importantes a nuestra consideración, sobre el contenido de las Directrices referidas.

1.4.1 Elaboración de perfiles.

Las Directrices sobre decisiones automatizadas defines a la elaboración de perfiles como:

> **"**Un procedimiento que puede implicar una serie de deducciones estadísticas. Suele usarse para hacer predicciones sobre personas, utilizando datos de distintas fuentes para inferir algo sobre un individuo o emitir un juicio, sobre la base de las cualidades de otros que parecen similares estadísticamente."[168]

1.4.2 Decisiones automatizadas.

Asimismo, considera que las decisiones basadas únicamente en el tratamiento automatizado representan "la capacidad de tomar decisiones por

---

[167]Grupo de Trabajo del Artículo 29, *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. Adoptadas el 3 de octubre de 2017. Revisadas por última vez y adoptadas el 6 de febrero de 2018.* Consultado el 18 de abril de 2019. Disponible en:
https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/wp251rev01_es-decisions-automatitzades.pdf

[168] *Ibidem*, p. 7:

medios tecnológicos sin la participación del ser humano en el proceso de decisión."[169]

El interesado tiene derecho a no ser objeto de este tipo de decisiones sin intervención humana, siempre que esta produzca efectos jurídicos o le afecte significativamente de modo similar.

Para ser considerada como intervención humana, el responsable del tratamiento debe garantizar que cualquier supervisión de la decisión sea significativa, en vez de ser únicamente un gesto simbólico.

> "Debe llevarse a cabo por parte de una persona autorizada y competente para modificar la decisión y como parte del análisis, debe tener en cuenta todos los datos pertinentes."[170]

En las Directrices también se define qué debemos entender por "efectos jurídicos" o "que afecte significativamente", para determinar si una decisión de esta naturaleza pone en riesgos los derechos del interesado:

> **"**Un efecto jurídico exige que la decisión, basada únicamente en el tratamiento automatizado, afecte a los derechos jurídicos de una persona, como la libertad de asociarse con otras personas, de votar en unas elecciones o de entablar acciones legales. Asimismo, un efecto jurídico puede ser algo que afecte al estatuto jurídico de una persona o a sus derechos en virtud de un contrato."[171]

Por otro lado, una decisión que le afecte significativamente de modo similar "es la que produce un efecto equivalente o significativamente similar en sus consecuencias a una afectación a los derechos."[172]

La elaboración de perfiles y las decisiones automatizadas ofrecen grandes beneficios en la economía digital. Las organizaciones, por ejemplo, pueden obtener beneficios como mayor eficiencia y ahorro de recursos, al permitir mediante procesos automatizados la toma de decisiones y las estrategias de

---

[169] *Idem.*
[170] *Ibidem,* p. 23.
[171] *Idem*.
[172] *Idem.*

mercadotecnia que deben implementar en determinados sectores o grupos de personas.

No obstante, la economía digital también presenta riesgos importantes a los derechos y libertades de las personas, debido a que estos procesos pueden ser en ocasiones opacos para los involucrados o las personas pueden no ser conscientes de que se está creando un perfil sobre ellas y no comprender lo que implica.

Uno de los principales riesgos observados sobre la elaboración de perfiles es que se pueden perpetuar estereotipos existentes y la segregación social. Asimismo, puede encasillar a una persona en una categoría específica y limitarla a las preferencias que se le sugieren.[173]

Esto puede socavar su libertad a la hora de elegir, por ejemplo, ciertos productos o servicios. En algunos casos, la elaboración de perfiles puede llevar a predicciones inexactas. En otros, puede llevar a la denegación de servicios y bienes, y a una discriminación injustificada. [174]

Si los datos utilizados en un proceso de decisión automatizada o de elaboración de perfiles son inexactos, cualquier decisión o perfil resultante puede estar viciado porque la información no corresponde con la realidad del interesado. Ocurre lo mismo con los datos desactualizados.

1.4.2.1 Inteligencia Artificial y *big data.*

La Inteligencia Artificial (IA) junto a *big data,* son elementos fundamentales en la toma de decisiones automatizadas y la elaboración de perfiles. Aunque ya se utiliza en muchas industrias, la IA está llamada a convertirse rápidamente en una parte integral de nuestra vida diaria.

Para Mark Purdy y Paul Daugherty:

> “La IA no es algo nuevo. Gran parte de sus fundamentos teóricos y tecnológicos fueron desarrollados en los últimos 70 años por científicos de la talla de Alan Turing, Marvin Minsky o John MacCarthy. En la Actualidad, este término hace referencia a diversas tecnologías que se pueden

[173] Cfr. Gil, Elena, *op.cit.,* pp. 124-129
[174] *Idem.*

combinar de distintas formas para sentir, comprender y actuar. Estas tres competencias se basan en la capacidad de aprendizaje a partir de la experiencia y la adaptación (*machine learning).* "[175]

Los mismos autores nos dicen, que hay dos factores clave para el crecimiento de la IA:

1. Acceso ilimitado a capacidad de procesamiento (la nube), y

2. Crecimiento del *Big Data*[176]

Big Data es el combustible de la Inteligencia Artificial (IA) mediante el cual los algoritmos se desarrollan. La IA puede tener distintas variantes como aprendizaje de máquinas (*machine learning*), aprendizaje profundo (*deep learning*) o robótica.[177]

En palabras de Barry Smyth, catedrático de informática en el University College de Dublín, "los datos son a la IA lo que la comida a los seres humanos. En un mundo cada vez más digital, el aumento exponencial de datos está llevando a constantes avances en la IA."[178]

Es evidente la correlación existente entre *big data* e IA, porque ambas se necesitan. La IA se nutre del *big data* para aprender, y el *big data* necesita la IA para extraer nuevas y mejores predicciones.[179]

Con esta información, podemos ver que, los algoritmos de IA se alimentan principalmente de toda la información que se almacena en "la nube" y del procesamiento de datos a través de *big data.* Con ello, cada día "aprende" más y es capaz de tomar más decisiones basadas en esta información y en la que genera.

En este sentido, la cantidad de datos, le permite generar, si es el caso, correlaciones que permitan a las organizaciones crear perfiles de personas muy

---

[175] Purdy, Mark y Daugherty, Paul, *Inteligencia Artificial, el futuro del crecimiento*, Accenture Institute for High Performance, 2016. Consultado el 5 de mayo de 2019. Disponible en: *https://www.accenture.com/t00010101t000000z__w__/es-es/_acnmedia/pdf-16/accenture_inteligencia_artificial_el-futuro-del_crecimiento_esp.pdfla=es-es*

[176] *Idem.*

[177] Riestra Herrera, Eduardo, *op.cit.,* p. 52.

[178] Purdy, Mark y Daugherty, Paul, *op.cit.* p.11.

[179] Riestra Herrera, Eduardo, *op.cit.,* p. 78.

exhaustivos y sólidos y tomar decisiones automatizadas basadas en complejos algoritmos, que solo un experto podría interpretar o entender.

Bajo esta tesitura, aunque la IA tiene múltiples beneficios en el crecimiento de la economía e innovación, es fundamental para el mundo del derecho generar leyes que se adapten a la IA, y con ello minimizar los riesgos de su mal uso.

En todo caso, el resultado de un algoritmo dependerá de cómo se gestiona y de qué información o datos personales se alimenta a la IA, por lo cual, es necesaria la intervención humana a fin de verificar previa y posteriormente a la toma de decisiones, que la información utilizada es correcta y actualizada y que no reproduce estereotipos existentes en las sociedades actuales.

En este sentido el RGPD propone que los responsables tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto.[180]

"El *big data* y los algoritmos pueden heredar o reflejar prejuicios y patrones de exclusión o ser resultado de quienes han tomado decisiones anteriores. Más allá de la intencionalidad que es muy posible que no se da en muchas ocasiones, se trata de un peligro objetivo que hay que prevenir"[181]

Al respecto, el Considerando 71 del RGPD establece que el responsable debe otorgar garantías adecuadas a la persona que es sometida a una decisión automatizada, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión.

[180] Considerando 71 del RGPD.

[181]Cotino Hueso, Lorenzo, "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata,* Valencia, España, Universidad de Valencia, año 2017, número 24. Consultado el 23 de abril de 2019. Disponible en : https://www.dilemata.net/revista/index.php/dilemata/article/view/412000104/494

La intervención humana es un elemento clave, toda revisión como se dijo, debe ser llevada a cabo por una persona con la autorización y capacidad adecuadas para modificar la decisión.

En este sentido, las personas que hacen uso de tecnologías disruptivas, deben hacer frente al riesgo de caer en conclusiones erróneas que nadie revisa, y prevenir el riesgo que para las personas pueda tener tomar decisiones automatizadas sin un sesgo humano.[182]

Bajo estas consideraciones, se debe tomar en cuenta que si la decisión promueve la reproducción de categorías de exclusión o actos discriminatorios que perpetúen los problemas de la "inteligencia humana" a la inteligencia artificial, es necesario volver a los principios básicos de la sociedad, y considerar a las personas en su dignidad humana y en el derecho a la igualdad.

Asimismo, las normas científicas y éticas son fundamentales, por lo que la creación de un marco ético común permite que quienes trabajan con este tipo de herramientas o tecnologías, actúen en favor de la humanidad.

1.5 Ejercicio de derechos en el RGPD.

El RGPD no establece un procedimiento para el ejercicio de derechos, sino que reconoce el derecho a la tutela judicial, al establecer en los artículos 77 a 82, que con independencia de los recursos administrativos o acción judicial, todo interesado tiene los siguientes derechos:

- Derecho a presentar una reclamación ante una autoridad de control
- Derecho a la tutela judicial efectiva contra la resolución vinculante de una autoridad de control[183]
- Derecho a la tutela judicial efectiva contra un responsable o encargado de tratamiento, sin perjuicio de que el interesado haya presentado una reclamación ante la autoridad de control.

[182] *Cfr.* Gil, Elena, *op.cit.* p. 32.

[183] En el Considerando 143 del RGPD se establece que tales decisiones se refieren en particular "al ejercicio de los poderes de investigación, corrección y autorización por parte de la autoridad de control o a la desestimación o rechazo de reclamaciones. No obstante, el derecho a la tutela judicial efectiva no incluye medidas adoptadas por las autoridades de control que no sean jurídicamente vinculantes, como los dictámenes publicados o el asesoramiento facilitado por ellas".

- Derecho a la indemnización y responsabilidad por daños o perjuicios (materiales o inmateriales).
- Derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro, que actúe en el ámbito de la protección de datos personales, presente en su nombre la reclamación, y ejerza en su nombre los derechos judiciales establecidos, así como el derecho a la indemnización.

Respecto a este último derecho, el RGPD considera que los Estados miembros pueden disponer que estas organizaciones, con independencia del mandado del interesado, tengan derecho a presentar reclamaciones en contra de la autoridad de control o del responsable o encargado, cuando existan motivos para creer que los derechos del interesado han sido vulnerados como consecuencia de un tratamiento.

Esta consideración es de gran ayuda para los interesados, debido a que sabemos que el ejercicio de los derechos que derivan del tratamiento de datos personales conlleva una carga que muchas veces el interesado no puede solventar o que, ante el uso global de plataformas en Internet, existe la posibilidad que el mismo tratamiento de datos afecte a muchas personas.

En este sentido, permitir la participación de asociaciones sin ánimo de lucro, que acompañen y representen a los afectados, es un avance en considerar la complejidad que presenta el ejercicio de este derecho.[184]

1.6 Límites a los derechos del interesado.

Es bien sabido que los derechos fundamentales no son de carácter absoluto, ni omnímodos en su ejercicio, como lo es el hecho de que su ejercicio quede condicionado en determinados supuestos, en aras de otros derechos tan estimables socialmente que ha merecido su elevación a rango constitucional.[185]

En este sentido, el RGPD expone de forma general en el Considerando 73 que el Derecho de la Unión o de los Estados miembros puede imponer

[184] Cfr. Contreras Zamora, Cristina, *¿Qué son las acciones colectivas en materia de protección de datos personales y porqué son importantes?,* México, Asociación Civil Artículo 12, 2019. Consultado el 26 de junio de 2019. Disponible en: *https://sontusdatos.org/2019/06/25/que-son-las-acciones-colectivas-en-materia-de-proteccion-de-datos-personales-y-porque-son-importantes/*
[185] Cfr. Del Castillo Vázquez, Isabel Cecilia, *op. cit.,* p. 469-470.

restricciones a determinados principios, derechos y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática y ajustarse a lo dispuesto en la Carta y en el Convenio Europeo.

Por su parte, el Tribunal Europeo de Derechos Humanos ha precisado que el contenido y los límites del derecho a la protección de datos personales dependen tanto del tipo de datos como de su utilización.[186]Por lo cual, los límites dependerán de cada caso en particular y de la prevalencia de un interés superior de la sociedad.

2. Obligaciones del responsable y encargado en el RGPD.

Consecuentemente, los derechos de los interesados se transforman en una obligación para el responsable o encargado.

En el caso del RGPD, el principio de responsabilidad proactiva es uno de los ejes sobre los que se construye la protección de datos personales, y tiene una estrecha relación con la aplicación por parte del responsable de medidas técnicas y organizativas apropiadas compatibles con la naturaleza, el ámbito, el contexto y los fines del tratamiento.[187]

En el RGPD se le da al responsable mayor control y libertad sobre el tratamiento, pero se le imponen obligaciones más estrictas, con un régimen sancionatorio más severo en caso de infracción.

A diferencia de la Directiva 95/46/CE donde las obligaciones se centraban en el responsable, en el RGPD tanto los responsables como los encargados deben cumplir con los principios y obligaciones expresas, acordes con su participación en el procedimiento.

2.1 Figura del responsable y encargado.

En el artículo 4 de definiciones se precisa al responsable, como “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento” y al encargado como “la

[186] Arenas Ramiro, Mónica, *op. cit.,* p. 80.
[187] Apartado 1, artículo 24 del RGPD.

persona física o jurídica que, por encargo del responsable, realiza el tratamiento de los datos"

La principal diferencia radica en la capacidad de decisión para determinar los fines y medios del tratamiento. Por un lado, el responsable (o corresponsables)[188] ostenta el control del tratamiento y determina qué datos se tratan, con qué finalidad y cómo serán tratados, sin necesidad de que él realice de forma directa el tratamiento de estos; por el otro, el encargado solo ejecuta las indicaciones del responsable y lleva a cabo el tratamiento en sentido estricto.

De esta manera, en primer término, se encuentran sujetos a la aplicación del RGPD, quien indica el cómo y porqué se procesan los datos personales, así como quien lleva a cabo el tratamiento en sí mismo, lo que permite que las obligaciones permeen todas las etapas del proceso.

2.2 Obligación de contar con un representante en la Unión

Como quedó establecido en el apartado del ámbito de aplicación, el RGPD incluye el tratamiento de datos personales de personas que se encuentren en la Unión, por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento tengan relación con la oferta de bienes o servicios a dichos interesados en la Unión o cuyo comportamiento esté siendo controlado.[189]

En este supuesto, el responsable o encargado tienen la obligación de designar un representante en la Unión, para atender principalmente las consultas por parte de las autoridades de control y del interesado sobre los asuntos relativos al tratamiento.

Dicha obligación no es aplicable en caso de tratamiento ocasional, que no incluya el manejo a gran escala de categorías especiales o el tratamiento realizado por las autoridades u organismos públicos. [190]

[188] Conforme al artículo 26 del RGPD, se consideran corresponsables del tratamiento, "cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento".
[189] Apartado 2, artículo 3 del RGPD.
[190] Artículo 27 del RGPD.

2.3 Implementar medidas de seguridad adecuadas

El Considerando 83 establece que a fin de mantener la seguridad y evitar que el tratamiento infrinja el RGPD, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas como el cifrado, para mitigarlos.

Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas**.**

Para tomar las medidas de seguridad de los datos, se deben tener en cuenta además, los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales."

En el mismo sentido, el artículo 32 instituye que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- La seudonimización y el cifrado de datos personales
- La capacidad de garantizar la confidencialidad, la integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de accidente físico o técnico
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

El Considerando 85 explica que la aplicación de medidas de seguridad adecuadas permite minimizar los efectos de lo ciberataques.

Así como evitar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación y pérdida de confidencialidad de datos sujetos al secreto profesional. [191]

Referimos antes, que medidas como la seudonimización no debe considerarse de forma aislada, sino en conjunto con otras medidas que permitan un nivel de seguridad adecuado, por lo que no ahondaremos en el tema.

2.4 La protección de datos desde el diseño y por defecto

Además de las medidas de seguridad que ambos deber prever, el responsable en particular tiene la obligación de tomar otras medidas tendientes a la protección del interesado que le proporciona sus datos personales, como la protección de datos desde el diseño y por defecto y las Evaluaciones de Impacto de Protección de Datos.

La protección de datos por diseño y defecto se encuentra en el artículo 25 del RGPD, donde se imprime la obligación del responsable del tratamiento de aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización.

Estas medidas están concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento.

La Agencia Española de Protección de Datos explica la protección de datos desde el diseño y por defecto en los siguientes términos:[192]

> “La protección de datos desde el diseño tiene como objetivo cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados y busca que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto.

[191] Cfr. Considerando 85 del RGPD.

[192]Agencia Española de Protección de Datos, *Medidas de protección de datos desde el diseño y por defecto*, Madrid, España. Consultado el 8 de junio de 2019. Disponible en: *https://www.aepd.es/reglamento/cumplimiento/privacidad-por-defecto.html*

Estos requisitos se van a traducir en medidas técnicas y organizativas con el objeto de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

El concepto de privacidad por defecto se refiere a que sólo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines".

Eduardo Riestra nos explica que, en la privacidad por defecto, la privacidad se mantiene salvaguardada sin necesidad de que las personas realicen ninguna acción para protegerla, por lo que los datos personales estarán por defecto protegidos en los sistemas IT (tecnología informática) o en las prácticas corporativas.

En la privacidad integrada desde el diseño, la privacidad formará parte del desarrollo técnico y funcional de los propios sistemas.[193]

Un ejemplo de cómo incorporar la protección de datos por diseño en la propia fase incipiente de desarrollo de un software sería definiendo en el mismo software el tiempo que los datos deben mantenerse según la norma legal aplicable, estableciéndose el procedimiento de borrado de forma automática cuando proceda.[194]

Un ejemplo de la protección de datos por defecto en las redes sociales es limitando desde el primer momento la accesibilidad del perfil de los usuarios para que por defecto no sea accesible a un número indefinido de personas.

En estos términos, la protección de datos deja de ser concebida como una tarea a posteriori para cumplir con la normativa aplicable, sino es un trabajo a priori, que debe formar parte fundamental en toda la realización de proyectos dentro de una organización.

2.5 Evaluación de impacto relativa a la protección de datos (EIPD)

Una evaluación de impacto es "un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del

[193] Cfr. Riestra Herrera, Eduardo, *op.cit.,* p. 19.
[194] *Ibidem*, p. 18.

tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos".[195]

Las evaluaciones de impacto conforme al artículo 35, serán obligatorias para el responsable del tratamiento cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

El tratamiento automatizado llevado a cabo con fines de la elaboración de perfiles y toma de decisiones automatizadas, así como tratamiento a gran escala de las categorías especiales de datos, son algunos de los tratamientos que el RGPD considera de alto riesgo, por lo cual, en estos casos, el responsable está obligado a la realización de una evaluación de impacto previamente.[196]

La evaluación de impacto se puede contemplar como una parte de la privacidad en el diseño porque anticipa al momento previo del tratamiento la previsión de las consecuencias de dicho tratamiento. [197]

2.6 Notificar violación de seguridad a la autoridad de control.

Una violación de seguridad de datos personales es "toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".[198]

Estas pueden clasificarse con arreglo a los siguientes tres principios de seguridad de la información: [199]

---

[195]Grupo de Trabajo del Artículo 29, *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. Adoptadas el 4 de abril de 2017. Revisadas por última vez y adoptadas el 4 de octubre de 2017.* Consultado el 27 de mayo de 2019. Disponible en: *https://www.aepd.es/media/criterios/wp248rev01-es.pdf*

[196]*Ibidem*, p. 9.

[197] Cfr. Riestra Herrera, Eduardo, *op.cit.* p. 35.

[198]Apartado 12, artículo 4 del RGPD.

[199]Grupo de Trabajo del Artículo 29, *Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679. Adoptadas el 3 de octubre de 2017. Revisadas por última vez y adoptadas el 6 de febrero de 2018, p. 8.* Consultado el 21 de mayo de 2019.Disponible en: *https://www.aepd.es/media/criterios/wp250rev01-es.pdf*

1. Violación de la confidencialidad. Cuando se produce una revelación no autorizada no accidental de los datos personales, o el acceso a los mismos.
2. Violación de la integridad. Cuando se produce una alteración no autorizada o accidental de datos personales.
3. Violación de la disponibilidad. Cuando se produce una pérdida de acceso accidental o no autorizada a los datos personales, o la destrucción de los mismos.

En términos del RGPD, en caso de que alguna de estas suceda, el responsable del tratamiento debe notificarla a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de los motivos de la dilación y se considera que el responsable tiene constancia de una violación, cuando tiene un grado razonable de certeza de que se ha producido un suceso que compromete los datos personales.[200]

La información que debe contener la notificación incluirá información como la naturaleza de la violación, las categorías de datos y de interesados afectados, descripción de las posibles consecuencias de la violación y de las medidas adoptadas o propuestas por el responsable para poner remedio a la violación y si procede, las medidas para mitigar los posibles efectos negativos.[201]

Para cumplir con lo anterior, los responsables tienen la obligación de documentar toda violación de seguridad, lo cual permitirá a la autoridad de control ejercer sus facultades de supervisión.

La notificación a la autoridad de control es indispensable en este punto, porque, de representar la violación de seguridad un alto riesgo para el interesado

[200] Grupo de Trabajo del Artículo 29, *Directrices sobre la notificación de las violaciones de la seguridad de los datos personales…, op.cit.,* p. 11.
[201] Artículo 33 del RGPD.

será esta, en su caso, quien obligue al responsable a que comunique al afectado las posibles consecuencias y las medidas que puede tomar para mitigar el daño.

De esta manera, aunque el responsable no cumpla con su obligación de informar al interesado, siempre quedará la figura de la autoridad de control para hacerlo cumplir el RGPD.

Asimismo, las autoridades de control cuentan con facultades para limitar el tratamiento, lo cual, puede prevenir que se continúe con el daño a los derechos del interesado.

2.7 Notificación de una violación de seguridad al interesado.

Conforme al artículo 34, cuando en un caso sea probable que la violación de seguridad pueda entrañar un alto riesgo para los derechos y libertades de los interesados, adicional a la notificación a la autoridad de control, el responsable debe también comunicarla a los interesados sin dilación indebida, así como incluir las recomendaciones para mitigar los potenciales efectos negativos.

Que una notificación se haga sin dilación indebida, significa que debe hacerse lo antes posible.[202]

Conforme a las Directrices sobre la notificación de violaciones de seguridad, el alto riesgo existe cuando la violación puede dar lugar a daños y perjuicios físicos, materiales o inmateriales para las personas cuyos datos han sido violados.

Ejemplos de tales daños y perjuicios son la discriminación, la usurpación de identidad o el fraude, la pérdida financiera y el daño para la reputación. Especialmente, cuando la violación se refiera a datos personales sensibles, se considerará probable que tales daños y perjuicios se produzcan.[203]

En las mismas Directrices, el G29 considera que notificar las violaciones de seguridad es una herramienta que mejora el cumplimiento respecto de la protección de los datos personales. En sentido contrario, el hecho de no informar puede convertirse en una sanción para el responsable del tratamiento. [204]

[202]Cfr. Considerando 85 del RGPD.
[203] Grupo de Trabajo del Artículo 29, *Directrices sobre la notificación de las violaciones de la seguridad de los datos personales…, op.cit.,* pp. 25 y 26.
[204]*Ibidem,* p. 6.

Para determinar si la violación entraña un alto riesgo para el interesado, se debe evaluar entre otras cosas, el tipo de violación, la naturaleza de los datos, la facilidad de identificación de las personas y gravedad y la permanencia de las consecuencias para las personas.[205]

En el caso de los datos biométricos, por ejemplo, no cabe duda del alto riesgo. Como se ha visto, estos, a diferencia de otros datos, (como el correo electrónico), no pueden ser remplazados por el interesado, por lo cual, la identidad de la persona afectada quedaría expuesta de manera específica y permanente.

2.8 Las autoridades de control en el RGPD.

Las autoridades encargadas de garantizar el derecho a la protección de datos personales son clave para proteger al titular de los datos, sobre todo, frente a los particulares.

El RGPD dota de facultades y poderes amplios a las autoridades de control al tomar en cuenta que son "un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal"[206].

En el artículo 51, se indica que una autoridad de control "es una autoridad pública, responsable de supervisar la aplicación coherente del Reglamento, con el fin de proteger los derechos y libertades fundamentales de las personas físicas en los que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión."[207]

Las funciones que desempeña una autoridad de control son:[208]

a) Controlar la aplicación del Reglamento y hacerlo aplicar
b) Promover la sensibilización del público y su comprensión, especialmente en niños, de las normas, derechos y riesgos en tratamiento de datos, así como promover la sensibilización de responsables y encargados respecto a sus obligaciones.
c) Asesorar a las autoridades y organismos sobre las medidas legislativas y administrativas relativas a los derechos y libertades de las personas

[205] *Ibidem,* pp. 26 a 29.
[206] Considerando 117 del RGPD.
[207] Artículo 51 del RGPD.
[208] Artículo 57 del RGPD.

d) Tratar e investigar las reclamaciones presentadas por los interesados o por un organismo u organización e investigar, e informar el curso de la investigación.
e) Cooperar con otras autoridades de control
f) Realizar investigaciones sobre la aplicación del Reglamento
g) Hacer seguimiento de cambios de interés, en la medida que puedan tener incidencia en la protección de datos, en particular el desarrollo de las TIC y las prácticas comerciales
h) Adoptar las cláusulas contractuales tipo, elaborar y actualizar el listado de evaluaciones de impacto, alentar la elaboración de códigos de conducta y mecanismos de certificación
i) Aprobar Normas Corporativas Vinculantes (NCV)
j) Llevar registro de las infracciones al RGPD
k) Desempeñar cualquier otra función relacionada con la protección de datos.

Adicional a enumerar las funciones de las autoridades de control, el RGPD prevé un listado sobre los poderes con que debe contar esta autoridad. Para ello, los divide en poderes de investigación, poderes correctivos y poderes de autorización y consultivos.

Los poderes de investigación son los siguientes:[209]

a) Ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;
b) Llevar a cabo investigaciones en forma de auditorías de protección de datos;
c) Llevar a cabo una revisión de las certificaciones expedidas
d) Notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

[209] Apartado 1 del artículo 58 del RGPD.

e) Obtener del responsable y del encargado del tratamiento el acceso a todos los datos e información necesaria para el ejercicio de sus funciones;
f) Obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos

Los poderes correctivos consisten en:[210]

a) Sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el Reglamento o con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;
b) Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado
c) Ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento
d) Ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;
e) Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición, cuando considere que es urgente intervenir para proteger los derechos y libertades del interesado
f) Ordenar la rectificación o supresión de datos personales o limitación de tratamiento, y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado
g) Retirar una certificación u ordenar al organismo de certificación que la retire
h) Imponer multas administrativas
i) Ordenar la suspensión de los flujos de datos a un país tercero u organización internacional

[210] Apartado 1, artículo 58 del RGPD

Los poderes de autorización y consultivos son:[211]

a) Asesorar al responsable conforme al procedimiento de consulta previa
b) Emitir dictámenes sobre cualquier asunto relacionado con la protección de datos
c) Autorizar el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular en relación con la protección social y la salud pública
d) Emitir un dictamen y aprobar proyectos de códigos de conducta de asociaciones u organismos representativos de responsables y encargados
e) Acreditar a los organismos de certificación, expedir certificaciones y aprobar criterios de certificación
f) Adoptar las cláusulas tipo de protección de datos, autorizar las cláusulas contractuales, los acuerdos administrativos y las NCV entre responsables y encargados como garantías adecuadas para las transferencias de datos.

Finalmente se deja a consideración de cada Estado dotar a la autoridad de control de otros poderes además de los indicados, y se menciona que debe contar con facultades para poner en conocimiento de las autoridades judiciales cualquier infracción al Reglamento y, si procede, iniciar o ejercer acciones judiciales.[212]

Para terminar, podemos concluir que las autoridades garantes deben vigilar el cumplimiento de la normatividad y en caso de incumplimiento aplicar el RGPD, que impone sanciones importantes con la finalidad de disuadir que se repita dicha situación.

En estos términos, cabe citar a Verónica López y Emilio Ontiveros que nos dicen:

> “El papel de los reguladores en el mundo de los datos es dual, ya que deben buscar el equilibrio entre la preservación de los derechos individuales de los usuarios y clientes, acotando los usos y comparticiones de datos

[211] Apartado 3, artículo 58 del RGPD
[212] Apartados 5 y 6, artículo 58 del RGPD.

entre empresas, y frenar con sus decisiones lo menos posible la capacidad de innovación, generación de valor y desarrollo de nuevas ideas por parte de empresas y emprendedores".[213]

3. Derechos del titular de los datos en la LFPDPPP

La LFPDPPP reconoce al titular de los datos el derecho de Acceso,[214] y dentro de este el derecho a conocer el Aviso de Privacidad al que está sujeto el tratamiento, el derecho de rectificación,[215] cancelación[216] y oposición[217] (Derechos ARCO). De forma incipiente se hace referencia a fundamentos del derecho al olvido y al derecho a no ser objeto de decisiones automatizadas.

Como el derecho de acceso y rectificación, en esencia, mantienen el contenido de instrumentos internacionales, y no contemplan ninguna novedad, no se incluirá su análisis en este apartado.

Por otro lado, sí retomaremos las consideraciones más importantes que establece la LFPDPPP respecto al derecho de cancelación, debido a que contiene de alguna manera el derecho al olvido, y el derecho de oposición, por ser considerados relevantes en la línea de análisis establecida en este trabajo.

3.1 Derecho de cancelación

"La cancelación implica el cese en el tratamiento por parte del responsable, a partir de un bloqueo de los mismos y su posterior supresión".[218]

"El titular podrá solicitar en todo momento al responsable la cancelación de los datos personales cuando considere que los mismos no están siendo tratados conforme a los principios y deberes que establece la LFPDPPP y el presente Reglamento. La cancelación procederá respecto de la totalidad de los datos personales del titular contenidos en una base de datos, o sólo parte de ellos, según lo haya solicitado".[219]

De resultar procedente la cancelación, el responsable deberá en términos del artículo 107 del Reglamento:

---

[213] López Sabater, Verónica y Ontiveros, Emilio, *op. cit.,* p. 71.
[214] Artículos 23 y 33 de la LFPDPPP y artículos 101 y 102 del Reglamento.
[215] Artículo 24 de la LFPDPPP.
[216] Artículos 25 y 26 de la LFPDPPP y artículos 105 a 108 del Reglamento.
[217] Artículo 27 de la LFPDPPP y artículos 109 a 111 del Reglamento.
[218] Artículo 105 del Reglamento.
[219] Artículo 106 del Reglamento.

"I. Establecer un periodo de bloqueo para impedir cualquier tratamiento, a excepción del almacenamiento, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de éstas,

II. Atender las medidas de seguridad adecuadas para el bloqueo,

III. Llevar a cabo el bloqueo en el plazo de quince días,

IV. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente".

Para Bertelson incluir el bloqueo como parte de la cancelación es un error.

"Este es un error, pues en todo caso debieran entenderse como derechos diferenciados, por un lado, la cancelación y por otro el bloqueo, pues la cancelación debe dar lugar a la destrucción del dato, mediante el mecanismo pertinente, mientras que el bloqueo "consiste en la facultad de exigir que se suspenda temporalmente el tratamiento de datos que estén almacenados, es decir que se suspenda cualquier operación…destinada a utilizar los datos en cualquier forma".[220]

En último término, la LFPDPPP no considera de forma explícita el derecho al olvido ni establece un procedimiento.

Pero se contempla como parte del derecho de cancelación la obligación del responsable de notificar a terceros a los que les haya transmitido la información la solicitud de cancelación, para que este, elimine los datos objeto de la solicitud de la base de datos en la que se encuentren, después de un plazo razonable.

Para Davara Fernández de Marcos:

"El concepto el derecho al olvido está fundado sobre instituciones jurídicas previas, como son la prescripción de delitos, la eliminación de antecedentes penales o las amnistías en temas financieros y fiscales.

[220]Bertelson Repetto, Raúl *et.al., Tratamiento de datos personales y protección de la vida privada, estudios sobre la Ley 19-628 sobre protección de datos de carácter Personal,* Santiago de Chile, Universidad de los Andes, Editor Jorge Wahl Silva, 2001, pp. 43-44. Consultado el 12 de mayo de 2019. Disponible en:
https://www.uandes.cl/wp-content/uploads/2019/03/Cuaderno-de-Extensi%C3%B3n-Jur%C3%ADdica-N%C2%B0-5-Tratamiento-de-Datos-Personales-y-Protecci%C3%B3n-de-la-Vida-Privada.pdf

Las normas de protección de datos que plantean los antes mencionados derechos ARCO dan la posibilidad al titular de los datos de que su información contenida en bases de datos, o, en términos generales, sometida al tratamiento, sea suprimida o cancelada."[221]

Como se ha dicho, el derecho al olvido tiene máxima relevancia cuando hablamos de motores de búsqueda en Internet, porque estos permiten obtener información sobre casi cualquier tema o persona, sin importar el tiempo transcurrido desde dicho suceso.

El Tribunal de Justicia de la Unión Europea en el caso de Google en 2014, determinó que es necesario garantizar que Internet sea un entorno seguro, en el que las personas tienen el derecho a permanecer anónimas, si así es su deseo.

En México es un derecho que forma parte del derecho de cancelación, por lo que solo es oponible frente al responsable del tratamiento. Ante ello, su ejercicio dependerá, si la ley lo permite, de a quienes se les considera como responsables del tratamiento en cada caso.

En la experiencia de la UE como hemos visto, se considera a los motores de búsqueda como responsables, aunque estos en sentido estricto no recogen los datos personales del interesado. Su responsabilidad nace al permitir el acceso a la información de forma estructura mediante la indexación.

En relación con el derecho de acceso a la información y libertad de prensa, el derecho al olvido tiene una cierta lucha, debido a que, en ocasiones, es reclamado por personajes políticos a los que se les ha señalado por estar envueltos en escándalos de ejercicio indebido del poder.

En un país con altos índices de corrupción como el nuestro, el derecho al olvido tiene que ser estudiado de una forma minuciosa y de forma conjunta con los derechos de acceso a la información, derecho a opinar y la libertad de prensa, por lo cual, se debe ponderar el valor de la información antes de emitir una resolución.

Si no se realiza en cada caso una evaluación del impacto que tiene eliminar información que forma parte de un evento de interés público, se empezará a ver al

[221] Davara Fernández de Marcos, Isabel, *op.cit.,* p. 34.

derecho al olvido como oportunidad para borrar la memoria histórica del país, y como se dice por ahí, quien olvida su historia, está condenado a repetirla.

3.2 Derecho de Oposición

El artículo 27 de la LFPDPPP establece que el titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos y de resultar procedente, el responsable no podrá continuar con el tratamiento de los datos relativos al titular.

Por su parte el Artículo 109 del Reglamento refiere que el titular podrá, en todo momento, oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo cuando:

> I. Exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular, o
>
> II. Requiera manifestar su oposición para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento para fines específicos.

En un primer momento puede confundirse con el derecho de cancelación, pero Tenorio Cueto nos explica que el derecho de oposición a diferencia de la cancelación no busca una supresión de los datos proporcionados, por el contrario, se consiente en proporcionarlos, pero se limita el tratamiento para fines específicos.

Desafortunadamente, la legislación mexicana no hace esta aclaración por lo que el derecho de oposición puede confundirse con el derecho de cancelación o bien, si se considera, con el derecho de bloqueo. [222]

La LFPDPPP no establece cuáles son los fines determinados a los que se puede oponer el titular de los datos, pero entenderemos que serán todos aquellos que son contrarios a la LFPDPPP o a la finalidad originaria, y que afectan al interesado por su situación específica.

[222] *Cfr.* Tenorio Cueto Guillermo Antonio *et.al.,* p. 64.

3.3 Ejercicio de los Derechos ARCO

El ejercicio de los derechos ARCO es parte fundamental en el derecho a la protección de datos personales.

Mediante este, el titular de los datos acude al responsable del tratamiento, para requerirle que le dé acceso a los datos, realice la rectificación de alguna información incorrecta o desactualizada, o para requerirle que cese en el tratamiento de los datos de forma total, o para determinados fines. Por ello, el ejercicio de estos debe ser accesible, sencillo y gratuito para el titular.[223]

El ejercicio de los derechos ARCO puede realizarse directamente por el titular de los datos o por medio de su representante legal en cualquier momento,[224] y se inicia a través de la presentación de una solicitud ante el responsable de los datos.

La solicitud deberá contener el nombre del titular, domicilio o medio para recibir notificaciones, los documentos que acrediten su identidad, una descripción clara y precisa de su solicitud y cualquier otro elemento que facilite la localización de sus datos.[225]

En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos.[226]

En caso de no recibir respuesta en los plazos establecidos o que esta no sea satisfactoria, el titular podrá presentar una solicitud ante el INAI.[227] La solicitud presentada es el único mecanismo que inicia el procedimiento de protección de datos por el Instituto.[228]

3.4 Decisiones sin intervención humana valorativa

Como tema olvidado en la LFPDPPP, es el Reglamento en su artículo 112 que recoge algunas consideraciones acerca del tratamiento de datos personales para la toma de decisiones sin intervención humana valorativa, al establecer que

[223] Artículo 35 de la LFPDPPP y artículo 93 del Reglamento.
[224] Artículos 22 y 28 de la LFPDPPP y artículo 89 del Reglamento
[225] Artículos 29, 31 y 32 de la LFPDPPP.
[226] Artículo 98 del Reglamento.
[227] Artículo 35 de la LFPDPPP.
[228] *Cfr.* Tenorio Cueto Guillermo Antonio *et.al., op.cit.,* p. 62.

el responsable debe informar al titular cuando se traten datos personales con esta finalidad.

En dado caso, el titular podrá ejercer su derecho de acceso, a fin de conocer los datos personales que se utilizaron para tomar la decisión correspondiente y, de ser el caso, el derecho de rectificación, cuando considere que alguno de los datos personales utilizados sea inexacto o incompleto.

De acuerdo con los mecanismos que el responsable tenga implementados para tal fin, el titular tiene la posibilidad de solicitar la reconsideración de la decisión tomada.

Las decisiones automatizadas es un asunto pendiente de desarrollar en la LFPDPPP. En primer lugar, queda imprecisa la forma y el momento en que se dará aviso al titular de los datos de que un tratamiento tiene como una de sus finalidades la toma de decisiones sin intervención humana valorativa.

Pensaríamos que, a través del aviso de privacidad, pero al retomar el contenido mínimo que debe prever el aviso de privacidad integral, que se considera el más completo, ninguna de sus fracciones establece que se deba informar al titular sobre estas decisiones y menos, sobre la elaboración de perfiles.

Siendo el aviso de privacidad el medio que la LFPDPPP reconoce por antonomasia para que el titular conozca la o las finalidades de un tratamiento, es contradictorio que no se incluya como parte esencial dicha notificación, y que se deje a consideración del responsable la forma de informar al titular.

En el mismo sentido, frente a estas decisiones, el titular solo puede ejercer el derecho de acceso o rectificación. El derecho de oposición que tiene la naturaleza de limitar el tratamiento para fines específicos que puedan causarle al titular de los datos un perjuicio por su situación particular, no está contemplado.

Aunque la intención de dotar al titular de los datos con un cierto tipo de derecho ante las decisiones automatizadas es muy buena, en la LFPDPPP no se logra concretar en una realidad y puede contrariamente tener un efecto negativo, al permitir este tipo de decisiones con base en esta normativa, pero sin garantías adecuadas al afectado.

Sin embargo, se tiene que considerar que la LFPDPPP referida fue publicada hace 9 años. La evolución de la tecnología sucede cada día, con nuevos medios y métodos para el procesamiento de información, y al derecho, más que a otras disciplinas, le cuesta seguirle el paso.

4. Obligaciones del responsable y encargado en la LFPDPPP

En el caso de México, más que obligaciones se establecen dos deberes que deberá cumplir el responsable, encargado y terceros que participen en el tratamiento: el deber de seguridad y el deber de confidencialidad.

Al igual que el RGPD, aunque el encargado y el responsable son obligados, será el responsable quien responderá por el cumplimiento de la LFPDPPP y responderá por el tratamiento.

Del mismo modo, la principal diferencia radica en el poder de decisión de cada uno. El responsable decide qué actividades se pueden realizar con los datos y el encargado se limita a ejecutar las acciones indicadas por el primero.

4.1 Deber de seguridad.

El deber de seguridad consiste en **"**establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra pérdida o destrucción, robo, extravío o copia no autorizada, uso, acceso o tratamiento no automatizado o el daño, la alteración o modificación".[229]

Para determinar las medidas de seguridad adecuadas a cada tratamiento, se debe tomar en cuenta principalmente el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.[230]

En caso de que se traten datos personales sensibles, las medidas deberán ser actualizadas cada año o cuando se vulneren los sistemas de tratamiento.[231]

La seguridad de la información es una garantía de la integridad, de la disponibilidad y de la confidencialidad,[232]por lo que el deber de seguridad deberá ser observado en todo el tratamiento.

---

[229] Artículo 63 del Reglamento.
[230] Artículo 19 de la LFPDPPP y 60 del Reglamento.
[231] Artículo 62 del Reglamento
[232] Cfr. Troncoso Reigada, Antonio, *op.cit.,* p. 1167.

La LFPDPPP no establece qué tipos de medidas deben adoptarse o cuáles parámetros seguir para elegir las que otorguen una clara seguridad de la información.

4.2 Deber de confidencialidad.

Obliga al responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales a guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.[233]

La confidencialidad pretende asegurar que solo las personas autorizadas tendrán acceso a la información.

Es asimilable al secreto de los médicos que tratan con datos sumamente sensibles relacionados con la salud de las personas. El secreto médico ha sido considerado tradicionalmente en su dimensión negativa, como un deber de reserva del profesional sanitario sin aceptar la vertiente positiva del mismo que atribuiría como contrapartida al paciente el derecho a exigir su cumplimiento[234]

Por lo cual, la confidencialidad, es un deber del responsable y un derecho del titular de los datos, que permite controlar el número de personas que tienen acceso a los datos personales.

Los deberes de seguridad y confidencialidad no son excluyentes, sino que se complementan, y ante la híper conectividad a través de dispositivos móviles, los responsables y encargados deben crear estrategias de ciberseguridad que les permitan garantizar la seguridad y confidencialidad de la información y demostrar el cumplimiento de sus obligaciones.

4.3 Notificación de vulneraciones de seguridad al titular de los datos

De conformidad con las Recomendaciones para el manejo de incidentes de seguridad de datos personales, emitidos por el INAI en junio de 2018,[235] un incidente de seguridad es “cualquier violación a las medidas de seguridad físicas,

[233] Artículo 21 de la LFPDPPP.
[234] Troncoso Reigada, Antonio, *op.cit.* p. 1177.
[235]INAI, *Recomendaciones para el manejo de incidentes de seguridad de datos personales,* México, 2018. Consultado el 11 de mayo de 2019. Disponible en: *http://inicio.ifai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pd*f

técnicas o administrativas de un responsable, que afecte la confidencialidad, la integridad o la disponibilidad de la información". [236]

Las vulneraciones a la seguridad de los datos personales o vulneraciones de seguridad son un tipo particular de incidente de seguridad, que se caracteriza por:[237]

a) Afectar a los activos o sistemas relacionados con los datos personales, en cualquier fase de su tratamiento, y

b) Afectar de manera significativa los derechos patrimoniales o morales de los titulares de los datos personales.

En el mismo sentido, el artículo 63 del Reglamento de la LFPDPPP considera al menos las siguientes vulneraciones:

I. La pérdida o destrucción no autorizada;

II. El robo, extravío o copia no autorizada;

III. El uso, acceso o tratamiento no autorizado, o

IV. El daño, la alteración o modificación no autorizada.

En caso de que ocurran estas vulneraciones de seguridad, en cualquier fase del tratamiento y afecten de forma significativa los derechos patrimoniales o morales de los titulares se debe informar de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.[238]

En esta notificación se le informará sobre la naturaleza del incidente, los datos comprometidos, recomendaciones acerca de las medidas que este puede adoptar, las acciones correctivas que han tomado y los medios para obtener más información.[239]

En este punto, a diferencia del RGPD, la obligación del responsable es únicamente de informar al titular de los datos, si este afecta de manera significativa sus derechos, no de notificar al INAI en cada caso de que exista un riesgo para los derechos de la persona.

---

[236] *Ibidem*, p. 6.
[237] *Ibidem,* p. 15.
[238] Artículos 20 y 64 del Reglamento.
[239] Artículo 65 del Reglamento.

En este sentido, la determinación de informar o no, recae únicamente sobre el responsable quien tiene amplia libertad de decidir si la violación de seguridad entraña un riesgo significativo para los derechos del titular, por lo cual, la persona que vea comprometida sus derechos por la vulneración de seguridad, muchas veces ni siquiera tendrá conocimiento de ello para tomar, de ser posible, alguna medida que mitigue los daños.

Por otro lado, llama la atención que, los responsables del sector público sí están obligados a notificar tanto al titular como al INAI las vulneraciones de seguridad dentro de un plazo máximo de 72 horas a partir de que se confirmen la ocurrencia de éstas.[240]

Esta es una muestra de los problemas que enfrenta la regulación dual que existe en nuestro país: obligaciones distintas que dependen de si el responsable es un particular o una autoridad.

4.4 Utilización de cómputo en la nube

La obligación del responsable radica, en utilizar solamente aquellos servicios en la nube en los que el proveedor garantice la debida protección de los datos personales, el cumplimiento de principios, el ejercicio de derechos y que cuente con medidas de seguridad adecuadas que garanticen la integridad y confidencialidad de los datos. **[241]**

El almacenamiento en la nube es un modelo de servicio en el cual los datos de un sistema de cómputo se almacenan, se administran, y se respaldan de forma remota, típicamente en servidores que están en la nube y que son administrados por un proveedor del servicio. Estos datos se ponen a disposición de los usuarios a través de Internet".[242]

Sabemos que el computo en la nube es un medio comprobado para lograr costos de capital más baratos y mejores capacidades operativas,[243]por lo cual, en

[240] Artículos 66 y 67 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el DOF el 26 de enero de 2018.
[241] Artículos 52 y 110 del Reglamento.
[242] Cfr. Téllez Valdés, Julio, *Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México,* México, UNAM, Instituto de Investigaciones Jurídicas, Editor Miguel López Ruíz, 2013, p. 5
[243] Cfr. Nava Garcés Alberto Enrique *et.al*., *op. cit.* p. 167.

proporción que las empresas aumentan el número de datos, tienen la necesidad de “mudarse” a la nube, para facilitar el almacenamiento de dicha información.

A medida que esto ocurre, hemos visto que varias configuraciones erróneas, falta de diligencia o mera indiferencia por parte de los administradores de este servicio, han dejado bases de datos expuestos públicamente en Internet para que cualquiera los vea y disponga de ellos, por lo que el tema de seguridad aún no se logra.

Uber Technologies Inc. (Uber), por ejemplo, ha estado involucrada en una serie de ataques cibernéticos en los últimos años, uno de los más importantes sufrido en 2016 y ocultado por la compañía hasta marzo de 2018.

A través de diversos medios de comunicación se dio a conocer que, en este accidente de ciberseguridad, le fueron robados millones de datos personales tanto de usuarios como de socios de todo el mundo.

En el caso de México, hasta hoy no se ha determinado de forma precisa, el número de usuarios afectados en México, o las acciones del INAI, principalmente, porque los centros de datos de Uber se encuentran en Estados Unidos, en cuyo caso, aunque se encontrara que era responsable por afectaciones a usuarios mexicanos, no se hubiera podido aplicar una sanción, y menos la reparación del daño.

En Estados Unidos, donde se ubica el domicilio de la empresa y sus servidores, se realizó todo un procedimiento de investigación, en el que se concluyó sancionar a la compañía por haber ocultado a sus clientes y a las autoridades el robo masivo de información. La sanción también contempló la obligación de Uber de hacer cambios en sus sistemas de seguridad para prevenir futuros ataques. [244]

Retomamos con esto, que la sociedad digital se desarrolla a través de espacios intangibles y los flujos de información traspasan las fronteras territoriales.

La idea que una oficina o establecimiento no tenga una ubicación física sino lógica y que los documentos e información que maneje se encuentren en

[244] Sobre el tema encontramos diversas notas periodísticas. Véase, por ejemplo, la nota del periódico El Financiero. Disponible en: *https://www.elfinanciero.com.mx/tech/uber-pagara-multa-historica-por-robo-de-datos*

servidores que puedan estar localizados en jurisdicciones diferentes a la de la ubicación del usuario o en “la nube” son conceptos revolucionarios para nuestro sistema jurídico.

Este nuevo paradigma de manejo de la información presenta importantes cuestiones de confianza para los usuarios.[245]

No obstante que la LFPDPPP tiene la virtud de obligar a cumplir el deber de seguridad y confidencialidad tanto al responsable como a terceros que intervengan en el tratamiento de datos personales, sin importar su grado de participación, no faculta a la autoridad encargada con facultades para actuar de manera activa en los procedimientos de protección de derechos.

El cómputo en la nube es por definición “ubicuo” y “transfronterizo”, pues el acceso a los recursos que facilita no depende de ninguna situación territorial, sino del acceso a Internet y sus características. En este sentido, su regulación debe ser acorde con la legislación a nivel mundial. [246]

Finalmente, se debe considerar que el poder de almacenamiento en la nube radica en su potencial para ofrecer un proceso estandarizado y simplificado que elimina las fronteras geográficas y físicas.

La innovación impulsada por la libertad de almacenamiento de datos en la nube radica en su capacidad para proporcionar dos atributos esenciales que proporcionan enorme flexibilidad: acceso en cualquier momento y desde cualquier dispositivo.

Su utilidad es importante en la economía digital, pero se debe tener en cuenta que la protección de los datos personales no es un tema que deba evadirse por problemas al momento de determinar la ubicación de los datos.

[245] Tenorio Cueto Guillermo Antonio *et.al.*, *op. cit.* p. 36.
[246] Cfr. Téllez Valdés, Julio, *op.cit.,* p. 14.

CAPÍTULO V. LEGISLACIÓN MEXICANA EN EL TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. RETOS Y PERSPECTIVAS ANTE EL NUEVO ESTÁNDAR EUROPEO.

1. Introducción

En México se han realizado acciones destacables encaminadas a la protección de datos personales.

Tal es el caso del reconocimiento a nivel constitucional como un derecho fundamental independiente del derecho a la vida privada, y la publicación de leyes reglamentarias.

El sistema de protección se diseñó de forma dual, por lo que se encuentran vigentes dos leyes en la materia: una es aplicable a entes públicos que realizan el tratamiento de datos personales y la otra aplicable a los particulares. Esta protección fragmentada que se aplica al mismo derecho resulta compleja en cuanto a su aplicación y observancia.

En este sentido, la estructura que garantiza el derecho humano a la protección de datos personales en nuestro país descansa en dos normas reglamentarias, y en una misma institución como organismo encargado de garantizar su cumplimiento: el INAI.

Para una mejor comprensión de este derecho en el contexto mexicano, y dirimir los retos que enfrenta el derecho a la protección de datos personales en posesión de particulares, después de analizar el contenido de la LFPDPPP correspondiente es necesario conocer a la Institución encargada de vigilar su cumplimiento.

Después de conocer ambos lados, tanto el contenido de la LFPDPPP como las facultades del INAI, observaremos de forma más clara porqué es necesario reformular tanto la legislación conforme al nuevo estándar europeo del RGPD y cómo las facultades del regulador deben ser más amplias para garantizar una protección efectiva frente a gigantes tecnológicos que dominan la economía de datos

2. INAI.

Como se ha mencionado, los organismos encargados de la defensa del derecho a la protección de datos personales tienen un papel determinante en la debida ejecución de la LFPDPPP.

Estos organismos, conforme a los estándares internacionales, deben ser especializados en el tema, independientes y contar con la capacitación técnica y jurídica que demanda el asunto ante el entorno digital.

El INAI es el organismo encargado en nuestro país de garantizar el derecho de acceso a la información y el derecho a la protección de datos personales.

Antes de ser un organismo autónomo, formó parte de la administración pública federal, por lo que recordaremos un poco de sus inicios para comprender mejor porqué actualmente enfrenta tantas limitaciones en la materia de protección de datos, sobre todo, frente a los particulares.

José Antonio Caballero nos cuenta que el entonces Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) se constituyó formalmente, mediante decreto presidencial publicado en el Diario Oficial de la Federación el 24 de diciembre de 2002, como un organismo descentralizado, no sectorizado, con personalidad jurídica y patrimonio propio.[247]

Es hasta el Decreto de reforma constitucional al artículo 6º en 2014, que se constituye como un organismo autónomo, responsable de garantizar el cumplimiento del derecho de acceso a la información pública ya la protección de datos personales en posesión de los sujetos obligados.

En el séptimo transitorio del mismo Decreto se estableció que mientras se determinaba la instancia encargada de atender los temas en materia de protección de datos personales en posesión de particulares, el organismo autónomo garante ejercería las atribuciones correspondientes. [248]

---

[247] Cfr. Caballero, José Antonio *et.al, El futuro del Instituto Federal de Acceso a la Información Pública y Protección de Datos Personales. Consideraciones sobre su autonomía constitucional,* México, UNAM, Instituto de Investigaciones Jurídicas, Centro de Investigaciones y Docencia Económicas, 2012, p. 6.

[248] Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, publicado en el DOF el 7 de febrero de 2014.

En cumplimiento del Decreto de reforma el otrora IFAI cambia su denominación por la de Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, y se le otorgan nuevas funciones como organismo garante a nivel nacional.

Si nos apegamos al texto de la reforma, podría decirse que el INAI, aunque es un organismo constitucional autónomo especializado, las facultades para conocer del derecho a la protección de datos personales en posesión de particulares, tienen carácter temporal, mientras se determina la instancia que se encargará de ello.

Posiblemente esta anotación es parte de que no se haya inscrito aún en el ADN de la institución la protección de datos personales frente a los entes privados como una prioridad.

Volviendo al tema, la autonomía del INAI derivó principalmente de la especialización que demandaba el tema y de la importancia que tomaban ambos derechos, acceso a la información y protección de datos, después de la reforma de 2011 en materia derechos humanos.

Como sabemos, los organismos autónomos se caracterizan por ser creados de forma directa por el texto constitucional; por contar con una esfera de atribuciones constitucionalmente determinada, porque no se encuentran orgánicamente adscritos o jerárquicamente subordinados a ningún otro órgano o poder, y debido a que llevan a cabo funciones esenciales dentro de los Estados modernos que demandan su especialización.[249]

En general, en el derecho y en la práctica política comparados se observa que los órganos constitucionales autónomos en primer término, pueden surgir por la necesidad de desarrollar funciones nuevas —normalmente más complejas— que el Estado no realizaba en tiempos pasados y que por sus características no pueden llevar a cabo los órganos incluidos en las tradicionales teorías de la división de poderes; y, en segundo lugar, por cuestiones coyunturales de un Estado, determinadas por necesidades particulares de la acción política.

[249] Cfr. Caballero, José Antonio *et.al., op.cit.,* p. 9-12.

Digamos que el INAI responde a ambas consideraciones. En materia de acceso a la información surge ante la necesidad social de conocer el ejercicio del poder público, y en protección de datos personales porque es un derecho que se desarrolla en casi todos los ámbitos de la vida económica, social y política de las sociedades actuales.

Bajo esta tesitura, el tema de protección de datos en las reformas que se han realizado siempre ha sido un tema controvertido, tanto por ser un derecho que en nuestro sistema se encuentra ligado al tema de transparencia en el ejercicio del poder público como por la evolución institucional del organismo garante.

El INAI encargado de proteger ambos derechos, se encuentra en un enclave de funciones en el que al parecer se procura primero el ejercicio del derecho a la información, que el derecho a la protección de datos personales, y más rezagado aún que la protección de datos en general, tenemos a la protección de este derecho frente a los particulares.

No obstante, el nacimiento al mundo jurídico de la LFPDPPP introduce nuevas atribuciones y condiciones en la operación del INAI que modifican, al menos en parte, la naturaleza de su actuación.[250]

Para estos efectos, la LFPDPPP dispone que el INAI tiene por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas y las que deriven de la misma. En particular aquellas relacionadas con el cumplimiento de obligaciones de los sujetos regulados.[251]

El artículo 39 de la misma LFPDPPP, fija las atribuciones del INAI en materia de protección de datos personales, entre las que destacan:

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

2. Interpretar en el ámbito administrativo la LFPDPPP;

[250] *Ibidem,* p. 8.
[251] Artículo 38 de la LFPDPPP.

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

4. Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en la LFPDPPP e imponer las sanciones según corresponda; y,

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

Las facultades más importantes del INAI en este listado de atribuciones es vigilar el cumplimiento de la LFPDPPP, y conocer del procedimiento de protección de derechos, procedimiento de verificación y del procedimiento sancionatorio.

Para efectos de este análisis veremos únicamente los dos primeros, porque, como hemos dicho, la aplicación de sanciones frente al poderío de los verdaderos responsables del tratamiento es un nivel al que difícilmente se llega.

3. Procedimiento de protección de derechos.

La LFPDPPP cuenta con una sección adjetiva dividida en tres tipos de procedimientos: procedimiento de protección de derechos, procedimiento de verificación y procedimiento de imposición de sanciones.

Conforme al artículo 45 de la LFPDPPP, el procedimiento de protección de derechos se inicia a instancia del titular de los datos o de su representante legal, frente al INAI, expresando con claridad el contenido de su reclamación y los preceptos de esta LFPDPPP que se consideran vulnerados, y es procedente únicamente bajo alguno de los siguientes supuestos:

1. Por falta de respuesta del responsable;
2. Cuando el responsable no entregue al titular los datos personales solicitados o lo haga en un formato incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, o
3. Cuando el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida.

Para el debido desahogo del procedimiento, el Instituto resolverá sobre la solicitud de protección de datos formulada, una vez analizadas las pruebas y

demás elementos de convicción que estime pertinentes, como pueden serlo aquéllos que deriven de la o las audiencias que se celebren con las partes.

El INAI tiene un plazo de 50 días para dictar la resolución, contado a partir de la fecha de presentación de la solicitud de protección de datos. Cuando haya causa justificada, podrá ampliar por una vez y hasta por un período igual este plazo.[252]

Si la resolución del INAI resulta favorable al titular de los datos, se requerirá al responsable para que, en el plazo de diez días siguientes a la notificación o cuando así se justifique, uno mayor que fije la propia resolución, haga efectivo el ejercicio de los derechos objeto de protección, debiendo dar cuenta por escrito de dicho cumplimiento al Instituto dentro de los siguientes diez días.[253]

El INAI podrá en cualquier momento del procedimiento buscar una conciliación entre el titular de los datos y el responsable. De llegarse a un acuerdo de conciliación entre ambos, éste se hará constar por escrito y tendrá efectos vinculantes y la solicitud de protección de datos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.

4. Procedimiento de verificación

A diferencia del procedimiento de protección de derechos, que requiere la acción por parte del titular de los datos o de su representante, el procedimiento de verificación puede iniciarse de oficio, o a petición de parte.

En términos del artículo 129 del Reglamento, cualquier persona podrá denunciar ante el Instituto las presuntas violaciones a las disposiciones previstas en la LFPDPPP y demás ordenamientos aplicables, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos.

El procedimiento de verificación iniciar de oficio bajo alguno de los siguientes supuestos: [254]

1) Cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos o,

[252] Artículo 47 de la LFPDPPP.
[253] Artículo 48 de la LFPDPPP.
[254] Artículo 59 de la LFPDPPP.

2) Cuando se presuma fundada y motivadamente la existencia de violaciones a la LFPDPPP.

El procedimiento de verificación a petición de parte, no se explica muy bien, pero conforme al artículo 22 del Reglamento cuando el responsable no permita al titular retirar el consentimiento para cesar el tratamiento de los datos, este puede presentar su solicitud ante el INAI para iniciar un procedimiento de verificación.

Es importante anotar respecto a ambos procedimientos que a diferencia de las resoluciones en materia de transparencia aplicables a entidades públicas[255], las resoluciones que derivan tanto del procedimiento de protección de derechos, como del procedimiento de verificación pueden ser impugnadas a través del juicio de nulidad.[256]

En estos términos, la resolución que emita el INAI en caso de ser impugnada será el otrora Tribunal Federal de Justicia Fiscal y Administrativa el encargado de revisarla (ahora Tribunal Federal de Justicia Administrativa).

No entraremos más al estudio de estos procedimientos porque como refiere Tenorio Cueto:

> "Es imperante precisar que no es propiamente un proceso de *Habeas data*, sino se trata de procedimientos que, aunque de manera material se nutran de lo pretendido por el *habeas data* respecto a la protección de los datos, carece de la intervención jurisdiccional y solo se limitan a ser procedimientos administrativos de carácter conciliatorio y sancionador."[257]

Etimológicamente, *habeas data* significa "conserva o guarda tus datos" (*habeas:* latín, *data:* inglés)[258] y su naturaleza es la de ser "un medio de protección constitucional, de carácter jurisdiccional, destinado a la salvaguarda de la libertad de la persona, en cuanto a su esfera informática.

Esto implica, reconocer el derecho de cualquier persona, para acudir a una instancia jurisdiccional, en caso de que sus datos personales, o los de su grupo familiar, se hayan visto modificados, afectados u alterados, para que estos sean

[255] Villanueva, Ernesto y Nucci, Hilda, *op.cit.* p. 266.
[256] Artículo 56 de la LFPDPPP y artículos 126 y 138 del Reglamento.
[257] Tenorio Cueto, Guillermo Antonio *et.al., op.cit.* p. 66.
[258] Villanueva, Ernesto y Nucci, Hilda, *op. cit.,* p. 184.

rectificados o suprimidos, según sea el caso, y, por ende, se concrete la reparación efectiva de tal vulneración.[259]

5. Panorama actual en México y propuestas

El panorama mexicano que hemos presentado después de este ejercicio comparativo con el nuevo estándar europeo que contiene el RGPD, nos lleva a concluir que los desafíos que presenta el sistema de protección de datos personales en posesión de particulares no son menores.

La Unión Europea en un referente en la materia, porque nos permite visualizar la importancia de regulaciones que sean aplicables de una forma más global.

La dualidad en la regulación (¿sobrerregulación?) crea una regulación asimétrica. Por un lado, la LGPDPPSO aplicable al sector público contiene disposiciones que garantizan de mejor manera la protección de los datos personales, que aquellas que se ubican en la LFPDPPP lo que afecta el derecho a igualdad jurídica y vuelve complejo el escenario de aplicación.

Por otro lado, aunque la LFPDPPP contempla muchos de los principios generales reconocidos a nivel internacional en la materia, su aplicación es todo un tema, sobre todo, cuando hablamos de plataformas internaciones que funcionan en Internet, que prestan servicios en México, pero llevan a cabo el tratamiento de los datos personales fuera del territorio mexicano.

Ejemplos de ello, empresas Google, Facebook y Uber, que, a decir de las sociedades actuales hiperconectadas, son los que realizan el mayor número de tratamientos de datos personales a nivel mundial.

En este sentido, retomando la experiencia europea, sería un gran avance recoger en una sola normatividad reglamentaria, la protección y garantía del derecho a la protección de datos personales; asimismo, establecer en esta que son sujetos obligados todas aquellas empresas que prestan servicios en el país y realizan el tratamiento de datos personales, con independencia de si cuentan con un establecimiento o no dentro del territorio, o de si el tratamiento se realiza dentro o fuera del país.

[259] Tenorio Cueto Guillermo Antonio *et.al., op. cit.,* p. 114.

Para ello, se puede imponer a los responsables que no residen en el país o tratan los datos fuera, la obligación de contar con un responsable en el país, que pueda responder por el tratamiento. Asimismo, es de máxima importancia la cooperación entre los Estados para lograr una protección adecuada en los flujos de información transfronterizos.

La LFPDPPP solo reconoce los derechos ARCO, y de forma escueta toma consideraciones del derecho al olvido y las decisiones basadas en un tratamiento automatizado.

Es necesario que se amplíe el reconocimiento de estos derechos ante tecnologías disruptivas como *big data* y la IA, no para limitar la innovación tecnológica y el crecimiento que estas herramientas permiten, sino para garantizar en todo momento que no se tornen en verdaderos métodos de discriminación y exclusión.

Por lo cual, es necesario reconocer nuevos derechos como el derecho a no ser objeto de decisiones basadas únicamente en un tratamiento automatizado sin que medie intervención humana, o el derecho a oponerse a la elaboración de perfiles cuando se coloque a las personas en categorías que reproducen estereotipos.

Asimismo, formular un verdadero derecho al olvido, que permita a la persona que lo ejerce borrar situaciones de su pasado, que permanecen en el tiempo gracias a la red, sobre todo en el caso de los niños y niñas, y reconocer el derecho a la información como elemento esencial para otorgar un consentimiento informado.

Los avisos de privacidad ya no deben tomarse como prueba plena de que el titular de los datos consiente tácitamente, por lo que hay que replantar la utilidad de estos y la utilidad que tienen si no son accesibles ni claros.

La LFPDPPP no impone obligaciones a los responsables y encargados del tratamiento, sino dos deberes: seguridad y confidencialidad.

En el deber no existe el constreñimiento de la LFPDPPP a cumplirla, es más un producto de actuar conforme a las normas. Adicionalmente, se deja a la autorregulación toda la carga de garantizar un tratamiento lícito y de respetar el

derecho a la protección de datos personales, cuando la autorregulación funciona como un mecanismo complementario para el cumplimiento de la LFPDPPP.

No queremos decir que se deben imponer cargas extras a los responsables del tratamiento, que restrinjan la necesaria circulación de datos en la economía digital, sino que es necesario una cierta actuación de la LFPDPPP en cooperación con mecanismos dentro de las organizaciones para responder ante los riesgos del tratamiento.

Pero también, existen obligaciones, como la privacidad por diseño y defecto, la responsabilidad proactiva y la transparencia, que deben apuntarse en la LFPDPPP, debido a que son imperativos necesarios en la adecuada gestión del derecho a la protección de datos, y sin los cuáles, no es posible el ejercicio de derechos.

Se podría, también, por ejemplo, imponer la obligación de notificar al INAI las vulneraciones de seguridad que afecten los derechos y libertades de las personas, lo que permitiría actuar desde la institución garante para mitigar el daño, y en su caso, lograr su reparación. De esta manera, no se deja a consideración del responsable determinado cuando una vulneración de seguridad afecta "significativamente" a los derechos de la persona.

Como se dijo antes, el establecimiento de un representante en el país que responda ante el titular de los datos y ante el INAI, es de gran utilidad en el tratamiento que se realiza fuera del país.

En los esquemas de autorregulación, se debe fomentar que los lineamientos emitidos por el INAI se consideren como parte de la legislación, no como meras recomendaciones que se pueden tomar en cuenta o no.

Asimismo, la participación del INAI debe ser activa, para revisar que estos mecanismos cuentan realmente como garantías adecuadas, y que no son emitidos solo como un método ilusorio de cumplimiento.

Finalmente, ante el poderío que ostentan quienes dominan el mercado tecnológico, es importante que se permita el ejercicio de acciones colectivas en estos casos, y permitir que asociaciones sin ánimo de lucro puedan iniciar un procedimiento ante el INAI cuando tengan cuenta de la afectación al derecho de

protección de datos personales por tratamientos ilícitos o vulneraciones de seguridad.

La naturaleza del INAI es ser garante de dos derechos: acceso a la información y protección de datos personales lo que ha dificultado su actuación, no solo porque son derechos con procedimientos distintos, sino, porque no permite que se vea al Instituto como un organismo especializado en la protección de datos, sino que pareciera una labor secundaria.

Su reputación es prácticamente conocida por los temas de transparencia, así que se debe trabar en ella como institución garante de la protección de datos personales.

Aunado, derivado del Decreto constitucional que lo faculta para conocer del derecho a la protección de datos personales frente a los particulares parece ser una tarea “temporal” mientras se crea un organismo que se encargue de ello, lo que, posiblemente ha colaborado a que no se inscriba en el ADN de la institución la protección de datos personales en posesión de particulares como una tarea principal.

Por lo cual, debería crearse un organismo especializado en el tema, o fortalecer las facultades del INAI en el tema, al determinar que no son “mientras” suceda otra cosa.

Los procedimientos de protección de derechos se inician únicamente a petición de parte, a diferencia de los procedimientos de verificación, lo que no permite al INAI contar con una legitimación activa en estos.

En este sentido, debería por lo menos otorgarse poderes suficientes al Instituto para que durante el desarrollo de los procedimientos pueda imponer algún tipo de medida cautelar, como es el caso de las autoridades de control en el RGPD que cuenta con facultades para obligar al responsable a la suspensión del tratamiento de manera temporal o definitiva, lo que evitaría que continuará la afectación a este derecho mientras el instituto resuelve.

A nivel doctrinal, los procedimientos establecidos en México no se tienen como verdaderas garantías del derecho a la protección de datos personales.

El *habeas data* permitiría acudir directamente a un órgano jurisdiccional para buscar la protección efectiva de los derechos como se encuentra reconocido en el RGPD, que con independencia de los procedimientos administrativas el interesado puede buscar la tutela judicial.

Adicionalmente, los procedimientos administrativos contemplados, como el juicio de nulidad, no estudian el fondo del asunto. Es decir, se pronunciará sobre la validez o nulidad del acto administrativo, pero no sobre el derecho a ejercer los llamados derechos ARCO.

Por lo que agotar un recurso administrativo ante el INAI, y dado el caso, ante el Tribunal, vulnera el derecho del titular de los datos de acceder a la justicia de forma pronta y expedita, lo que deja de manifiesto, que el derecho a la protección de datos personales frente a los particulares no se entiende como un auténtico derecho humano.

El procesamiento automatizado de datos es algo que ocurre y cambia en cuestión de segundos. Cuando el titular por fin obtenga una resolución favorable, si es el caso, la afectación posiblemente ya se habrá concretado o las situaciones se habrán modificado a tal punto que no sea posible determinar si persiste o no la situación que dio origen al ejercicio de los Derechos ARCO.

Retomamos que, si se tiene a los procedimientos como garantías no jurisdiccionales del derecho a la protección de datos personales, debería el INAI tener la facultad de imponer en aquellos casos que sea necesario una medida que detenga la vulneración del derecho, como la suspensión temporal del tratamiento.

Así, aun cuando el procedimiento sea largo seguirá su desarrollo sin causar más afectaciones al titular.

En caso contrario, se deben crear mecanismos jurisdiccionales que permitan el acceso a la justicia de forma pronta y expedita. Del mismo modo, la LFPDPPP debe prever garantías suficientes para el ejercicio de los derechos del titular de los datos frente a los responsables del tratamiento, como las empresas digitales, que representan una barrera infranqueable para el usuario normal.

Para terminar, solo nos queda decir que el INAI, como autoridad encargada de la protección de datos personales en posesión de los particulares (por ahora) a

partir de la reforma de 2014, hace grandes esfuerzos por garantizar la protección de este derecho en el entorno digital, pero en diversas ocasiones ante vulneraciones de seguridad que sufren las grandes empresas digitales, el INAI no puede aplicar la LFPDPPP, porque sus facultades se encuentran limitadas.

Primero, porque la LFPDPPP solo es aplicable en territorio nacional, segundo, porque el INAI funciona como un organismo pasivo ante el procedimiento de protección de derechos, que requiere una actuación previa por parte el titular de los datos, para que sea posible iniciarlo, y tercero, porque la naturaleza del INAI lo hace autoridad garante tanto del derecho de acceso a la información y de manera secundaria, del derecho a la protección de datos personales.

En este orden de ideas, no solo es necesario formular reformas a la LFPDPPP, sino crear un organismo con poderes suficientes para hacer valer la ley frente a los particulares que vulneren el derecho fundamental a la protección de datos personales.

CONCLUSIONES

El derecho a la protección de datos personales es un derecho ligado a la intimidad, a la vida privada, y a otros derechos, pero es un derecho independiente porque no necesita una afectación a otro derecho para ser ejercicio. Es también un derecho digital, es decir, crece y se desarrolla junto a las sociedades híper conectadas.

Toma especial atención el derecho a la protección de datos personales, porque en la economía digital, los datos son vistos como un insumo esencial y funcionan como moneda de cambio en todas las interacciones que tenemos con Internet, que sumado a las nuevas tecnologías emergentes permite el tratamiento masivo de datos personales de forma ubicua y deslocalizada.

No obstante este nuevo "uso", se debe tener en cuenta que los datos son de su titular, no como una relación o un derecho de "propiedad", sino un derecho personalísimo, como el derecho al honor, a la intimidad y a la propia imagen. Por lo cual, aunque los datos se utilicen en transacciones en línea o sean compartidos con otra persona para que esta los "trate", no significa que se cede el control sobre ellos.

En este sentido, no basta con que el derecho a la protección de datos personales sea reconocido como un derecho fundamental independiente, sino que es necesario crear mecanismos jurídicos e institucionales *ad hoc* para protegerlo, que permitan la prevención, la sanción o la reparación efectiva, y que fomente la libre circulación, en favor de la economía digital, pero con las garantías adecuadas.

Para lograrlo, los mecanismos de protección pueden ser jurisdiccionales o no jurisdiccionales, pero deben ser coherentes e interoperables a nivel internacional y efectivos como garantías adecuadas en la protección de este derecho.

Los organismos garantes son fundamentales en el logro de esta finalidad. Por lo cual deben estar dotados de poderes suficientes para aplicar la LFPDPPP y sancionar su incumplimiento, así como estar capacitados técnica y jurídicamente

para reconocer las implicaciones de la tecnología en la protección de datos personales.

De no ser así, se produciría un efecto adverso, donde se obstaculice la innovación tecnológica y no se proteja de manera adecuada y efectiva el derecho fundamental a la protección de datos personales.

En conclusión, es necesario crear un organismo especializado o fortalecer las facultades del regulador y fomentar su capacitación técnica; actualizar la legislación para que responda a los nuevos retos de la economía de datos, garantizar el ejercicio de derechos a través de mecanismos adecuados sean jurisdiccionales o no, así como promover el uso de los datos personales de manera responsable en favor del crecimiento económico.

El derecho no debe permanecer ajeno a la relación dialéctica que existe entre el derecho a la protección de datos personales y la tecnología, de lo contrario, se caería en el error de emitir legislaciones que no sean aplicables a la realidad de la sociedad digital, lo que obstruye el camino para capitalizar de forma segura las transformaciones que trae la revolución tecnológica.

FUENTES DE CONSULTA

ANDREU MARTÍNEZ, Ma. Belén, *La protección de datos personales de menores de edad*, Navarra, España, Editorial Aranzandi SA, 2013.

ARENAS RAMIRO, Mónica, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, España, Editorial Tirant Lo Blanch, 2006.

CABALLERO, José Antonio *et.al.,El futuro del Instituto Federal de Acceso a la Información Pública y Protección de Datos Personales. Consideraciones sobre su autonomía constitucional,* México, UNAM, Instituto de Investigaciones Jurídicas, Centro de Investigaciones y Docencia Económicas, 2012.

CAMPUZANO TOMÉ, Herminia, *Vida privada y datos personales*, España, Editorial Tecnos, 2000.

DAVARA FERNÁNDEZ DE MARCOS, Isabel, *El derecho al olvido en relación con el derecho a la protección de datos personales*, México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2014.

DEL CASTILLO VÁZQUEZ, Isabel Cecilia, *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, Pamplona, España, Editorial Arazandi, 2007.

GIL Elena, *Big data, privacidad y datos personales*, Madrid, España, Agencia Española de Protección de Datos, 2016.

GONZÁLEZ PADILLA, Roy, *Cuadernos de trabajo. Posesión de datos personales en posesión de particulares,* México, Senado de la República, 2011.

GOZAÍNI, Osvaldo, *Derecho procesal constitucional, habeas data, protección de datos personales,* Buenos Aires, Argentina, Editorial Rubinzal-Culzoni Editores, 2001.

HIDALGO RIOJA, Ileana, *Derecho a la protección de datos personales*, México, INEHRM, UNAM, Instituto de Investigaciones Jurídicas, 2018.

LÓPEZ RUÍZ, Miguel, *Redacción legislativa*, México, Senado de la República, 2002.

LÓPEZ SABATER VERÓNICA, Ontiveros Emilio, *Economía de los datos. Riqueza 4.0,* Madrid, España, Editorial Ariel, 2017.

LORENZO CABRERA, Sara *et.al., Protección de datos, responsabilidad activa y técnicas de garantía. Curso de "delegado de protección de datos" adaptado a la nueva Ley orgánica 3/2018 de 5 de diciembre de protección de datos personales y garantía de los derechos digitales*, Madrid, España, Editorial Reus, 2018.

NAVA GARCÉS, Alberto Enrique *et.al., El derecho en la era digital. Internet, firma electrónica, protección de datos, delitos informáticos, comunicaciones, redes sociales, preservación de evidencia*, México, Editorial Porrúa, 2013.

PALAZZI A, Pablo, *La transmisión internacional de datos personales y la protección de la privacidad. Argentina, América Latina, Estados Unidos y La Unión Europea*, Editorial Adhoc, Buenos Aires, Argentina, 2002.

PIÑAR MAÑAS, José Luis, *¿Existe la privacidad?*, Madrid, Editorial CEU ediciones, 2008.

RECIO GAYO, Miguel, *La protección de datos en el ámbito de las telecomunicaciones e Internet,* México, México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, diciembre 2015.

RIESTRA HERRERA, Eduardo, *Privacidad en el Diseño de la Inteligencia Artificial*, España, Asociación de Marketing de España, 2017.

ROIG, Antoni, Derechos fundamentales y tecnologías de la información y de las telecomunicaciones (TIC), Barcelona, España, Editorial JMBosch, 2010.

RUÍZ MIGUEL, Carlos, *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Madrid, España, Editorial Civitas, 1994.

TÉLLEZ CARBAJAL, Evelyn (coord.), *Derecho y TIC. Vertientes actuales*, México, UNAM, Instituto de Investigaciones Jurídicas, INFOTEC, 2016.

TELLEZ VALDÉS, Julio, *Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México,* México, UNAM, Instituto de Investigaciones Jurídicas, 2013.

TENORIO CUETO Guillermo *et.al., Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares,* México Editorial Porrúa, 2010.

TRONCOSO REIGADA Alonso, *La protección de datos personales. En busca del equilibrio*, Valencia, España, Editorial Tirant Lo Blanc, 2010.

VILLANUEVA, Ernesto y Nucci, Hilda, *Comentarios a la Ley Federal de Protección de Datos Personales en Posesión de Particulares*, México, Editorial Liber Iuris Novum, 2012.

Artículos electrónicos.

ÁLVAREZ CARO, María, "Reflexiones sobre la sentencia del TJUE en el asunto 'Mario Costeja' (C-131/12) sobre derecho al olvido", *Revista Española de Derecho Europeo*, núm. 51.Disponible en:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Universidad Politécnica de Madrid, Análisis de los flujos de información en Android. Herramientas para el cumplimiento de la responsabilidad proactiva, Madrid, España, 2019. Disponible en: *https://www.aepd.es/media/estudios/estudio-flujos-informacion-android.pdf*

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Protección de Datos: Guía para el ciudadano*, Madrid, España, 2018.

Disponible en*: https://www.aepd.es/media/guias/guia-ciudadano.pdf*

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía sobre el uso de las cookies,* p.7. Disponible en:

http://www.interior.gob.es/documents/10180/13073/Guia_Cookies.pdf/7c72c988-1e55-42b5-aeee-f7c46a319903

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Medidas de protección de datos desde el diseño y por defecto. Disponible en:

https://www.aepd.es/reglamento/cumplimiento/privacidad-por-defecto.html

ASOCIACIÓN CIVIL ARTÍCULO 12, *¿Qué son las acciones colectivas en materia de protección de datos personales y porqué son importantes?,* Ciudad de México, México, 2019. Disponible en:*https://sontusdatos.org/2019/06/25/que-son-las-acciones-colectivas-en-materia-de-proteccion-de-datos-personales-y-porque-son-importantes/*

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD, *Los principios generales de la protección de datos, ¿Fundamentos y/o deberes?*, España, 2018. Disponible en: *https://dpd.aec.es/los-principios-generales-la-proteccion-datos-fundamentos-deberes/*

COMISIÓN EUROPEA, Dirección General de Justicia y Consumidores, *La reforma de la protección de datos en la UE y los macrodatos*. *Ficha informativa,* 2016. Disponible en:
https://publications.europa.eu/es/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1
BERTELSON REPETTO, Raúl, "Tratamiento de datos personales y protección de la vida privada" en Cuadernos *de extensión jurídica,* Santiago de Chile, Universidad de los Andes, número 5, 2001. Disponible en:
https://www.uandes.cl/wp-content/uploads/2019/03/Cuaderno-de-Extensi%C3%B3n-Jur%C3%ADdica-N%C2%B0-5-Tratamiento-de-Datos-Personales-y-Protecci%C3%B3n-de-la-Vida-Privada.pdf
COMISIÓN EUROPEA, Dirección General de Justicia y Consumidores, *La reforma de la protección de datos en la UE y los macrodatos*, 2016. Disponible en *https://publications.europa.eu/es/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1*
COTINO HUESO, Lorenzo, "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales, *Dilemata*, Valencia, España, año 2017, número 24. Disponible en:
https://www.dilemata.net/revista/index.php/dilemata/article/view/412000104/494
DEL ÁLAMO, José María *et.al., Análisis de los flujos de información en Android. Herramientas para el cumplimiento de la responsabilidad proactiva,* Madrid España, Agencia Española de Protección de Datos, Universidad Politécnica de Madrid, 2019. Disponible en:
https://www.aepd.es/media/estudios/estudio-flujos-informacion-android.pdf
FLORES, María Victoria, "La globalización como fenómeno político, económico y social", *Orbis,* Maracaibo, Venezuela, 2016, vol. 12, núm. 34.
Disponible en *http://www.redalyc.org/articulo.oa?id=70946593002*
Gamboa Montejano, Claudia, *Datos personales. Estudio Teórico Conceptual, de su regulación actual y de las iniciativas presentadas para la creación de una Ley en la materia (Primera Parte),*México, Cámara de Diputados LXI Legislatura, Centro de Documentación, Información y Análisis, 2009.

Disponible en:*http://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-24-09.pdf*

Google, *Centros de Datos.* Disponible en: *https://www.google.com/intl/es-419/about/datacenters/gallery/index.html#/places*

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. Adoptadas el 3 de octubre de 2017. Revisadas por última vez y adoptadas el 6 de febrero de 2018.*Disponible en: *https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/wp251rev01_es-decisions-automatitzades.pdf*

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 adoptadas el 28 de noviembre de 2017 revisadas por última vez y adoptadas el 10 de abril de 2018.* Disponible en: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051*

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. Adoptadas el 4 de abril de 2017. Revisadas por última vez y adoptadas el 4 de octubre de 2017.* Disponible en: *https://www.aepd.es/media/criterios/wp248rev01-es.pdf*

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre la transparencia en virtud del RGPD 2016/679. Adoptadas el 29 de noviembre de 2017. Revisadas por última vez y adoptadas el 11 de abril de 2018.* Disponible en:*https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/wp260rev01_es-transparencia.pdf*

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679. Adoptadas el 3 de octubre de 2017. Revisadas por última vez y adoptadas el 6 de febrero de 2018.* Disponible en: *https://www.aepd.es/media/criterios/wp250rev01-es.pdf*

INSTITUTO IMDEA NETWORKS, Universidad Carlos III de Madrid, *An Analysisof Preinstalled Android Software*, Madrid, España, 2019. Disponible en:*https://haystack.mobi/papers/preinstalledAndroidSW_preprint.pdf*

INAI, *Recomendaciones para el manejo de incidentes de seguridad de datos personales,* México, 2018. Disponible en:
http://inicio.ifai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

INAI, *Guía para la configuración de privacidad en redes sociales*, México, 2018. Disponible en: *http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF*

OCDE/BID, *Políticas de banda ancha para América Latina y el Caribe: un manual para la economía digital, OECD,* Paris, 2016.
Disponible en: *http://dx.doi.org/10.1787/9789264259027-es*

PARLAMENTO EUROPEO, *La protección de los derechos fundamentales en la Unión Europea,* 2019. Disponible en:
www.europarl.europa.eu/ftu/pdf/es/FTU_4.1.2.pdf

PARLAMENTO EUROPEO, *El mercado único digital omnipresente*, 2019. Disponible en: *http://www.europarl.europa.eu/ftu/pdf/es/FTU_2.1.7.pdf*

UBER, *Política de Privacidad.* Disponible en: *https://privacy.uber.com/policy*

PURDY Mark, Daugherty Paul, I*nteligencia Artificial, el futuro del crecimiento*, Accenture Institutefor High Performance, 2016. Disponible en:
https://www.accenture.com/t00010101t000000z__w__/es-es/_acnmedia/pdf-16/accenture_inteligencia_artificial_el-futuro-del_crecimiento_esp.pdfla=es-es

SÁNCHEZ DEL CAMPO, Alejandro, “Reflexiones de una replicante legal: los retos jurídicos de la robótica y las tecnologías disruptivas”, *AAKAT: Revista de Tecnología y Sociedad,* Navarra, España, 2016.Disponible en:
http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/383

SZPUNAR, Maciej, Abogado General, Tribunal de Justicia de la Unión Europea, *CONCLUSIONES DEL ABOGADO GENERAL SR. MACIEJ SZPUNAR presentadas el 10 de enero de 2019 (1), Asunto C‑507/17, Google LLC, que se ha subrogado en los derechos de Google Inc. contra Commissionnationale de l’informatique et des libertés (CNIL), con intervención de Wikimedia Foundation Inc., Fondationpour la liberté de la presse, Microsoft Corp., ReportersCommitteeforFreedomofthePress y otros, Article 19 y otros, Internet*

FreedomFoundation y otros, Défenseur des droits, 2019. Disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62017CC0507&qid=1565060402063&from=EN*

Legislación mexicana

Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, publicado en el DOF el siete de febrero de dos mil catorce

Decreto por el cual se adiciona un segundo párrafo con siete fracciones al artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, publicado en el DOF el 20 de julio de 2007.

Decreto por el cual se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el DOF el 1 de junio de 2009.

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

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

Lineamientos del Aviso de Privacidad

Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Legislación europea.

Carta de Derechos Fundamentales de la Unión Europea.

Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal de 1981(Convenio 108 del Consejo de Europa).

Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

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)