LEY FEDERAL
DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES, COMENTADA

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Guillermo A. Tenorio Cueto
Coordinador Editorial

LEY FEDERAL
DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES, COMENTADA

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

DIRECTORIO

COMITÉ EDITORIAL

Las opiniones expresadas en esta publicación son responsabilidad exclusiva de los autores y no reflejan necesariamente las del INAI.

Insurgentes Sur 3211, colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, Ciudad de México, C.P. 04530.
Tiraje: 2,000 ejemplares.
ISBN: 978-607-98648-1-1

Primera edición, octubre de 2019.
Impreso en México, *Printed in Mexico.*
Ejemplar de distribución gratuita.

ÍNDICE

PRESENTACIÓN

Desde que nacemos hasta nuestra muerte generamos información que da cuenta de nuestra existencia: dónde nacimos, quiénes son nuestros padres, dónde estudiamos, qué gustos tenemos, dónde trabajamos, cuánto dinero tenemos, qué lugares frecuentamos, imágenes, sonidos y demás información que nos hacen identificables. Todos esos datos personales nos describen. Actualmente, con el uso de las tecnologías se pretende predecir posibles comportamientos, evaluar nuestros gustos y preferencias, así como mejorar mecanismos para vendernos bienes, productos o servicios.

Por ello, cada vez más, las empresas están interesadas en conocer la mayor cantidad de información sobre nosotros. Hoy, más que nunca, nuestra información y datos personales tienen valor. No sólo como mera apreciación afectiva, sino como un valor económico y cuantificable en el mercado.

El desarrollo jurídico de la protección de los datos personales en México es relativamente reciente. No obstante, desde los antecedentes de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (ya derogada), pasando por las reformas de los artículos 16 y 73, fracción XXIX-O constitucionales de 2009, que se tradujeron en la publicación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, el 5 de julio de 2010, se han tenido avances significativos.

Una de las preocupaciones más importantes de los legisladores durante la discusión de esta ley fue el contexto de inseguridad y la relevancia de proteger la información personal de los mexicanos que es tratada, tanto por autoridades como por particulares. En la revisión de la discusión encontramos alusiones a la facilidad con la que podían adquirirse bases de datos del padrón electoral, del parque vehicular, incluso de los archivos de policía.

Estas bases de datos solían ser adquiridas, de acuerdo con investigaciones periodísticas, por cualquier persona, con fines mercadológicos, en el mejor de los casos. La entrada en vigor de la Ley Federal de Protección de Datos Personales en Posesión de Particulares pretendía poner fin a esta situación.

A la par, en los debates legislativos se destacó el hecho de que con la aprobación esta ley, México se colocaba a la altura de los países miembros de

la OCDE, la APEC y de la Unión Europea, pues cumpliría con los estándares internacionales en materia de privacidad aprobados en la Conferencia Mundial de Comisionados de Privacidad y Protección de Datos, que se llevó a cabo en noviembre de 2009.

En la presente obra se emiten comentarios que los autores consideran relevantes para la interpretación de la ley. El análisis se presenta por capítulos para no fraccionarlo y reducir el número de remisiones entre las normas, ya que los capítulos de la Ley Federal de Protección de Datos Personales se encuentran organizados temáticamente.

Al mismo tiempo, en cada capítulo se incluye un útil apartado denominado "correlaciones" que permite identificar, de manera rápida, los artículos del Reglamento de la Ley que se relacionan con cada uno de los temas abordados. Dependiendo de estos, en algunos capítulos se realizó una relación de normativa más detallada que puede incluir, incluso, lineamientos o guías emitidas por el INAI en cada una de las materias. Este ejercicio de correlación facilita el cumplimiento de la Ley para los responsables, al permitirles conocer qué normas deben aplicar en cada caso y cómo hacerlo.

Además de realizar un análisis de las disposiciones de la Ley Federal de Protección de Datos Personales, los autores también expresan algunas observaciones que ponen en evidencia importantes áreas de oportunidad para la actualización de esta Ley. Si bien, al momento de su promulgación y publicación en el *Diario Oficial de la Federación* se cumplía con los estándares internacionales aplicables, no debemos perder de vista que el marco jurídico internacional ha evolucionado, mientras que nuestra Ley ha permanecido sin adecuación alguna. En este sentido, la presente obra es de interés y relevancia, no sólo para los sujetos regulados que deben cumplir con la Ley, sino también para aquellos interesados en los procesos legislativos.

Mucho se ha avanzado desde la promulgación de la Ley, sólo por señalar algunos datos, en 2012 se presentaron 50 quejas (procedimiento de protección de derechos) ante el entonces IFAI por inconformidad con la atención que se dio a la solicitud de acceso, rectificación, cancelación u oposición al tratamiento de datos personales, mientras que en 2018 se recibieron 251 reclamos. Solamente en seis años aumentaron más de 400 por ciento las personas que confiaron en el INAI como vía para garantizar su derecho a la autodeterminación informativa.

Adicionalmente, las verificaciones iniciadas (ya sea por denuncia o de manera oficiosa) se incrementaron drásticamente al pasar de ocho procedimientos en 2012 a 667 en 2018. Como resultado de estas, o bien por incumplir resoluciones del INAI, el pleno ha emitido 354 resoluciones donde se sancionaron a particulares (personas físicas o morales) por incumplir con las disposiciones de esta Ley.

Aún queda un vasto camino por recorrer. Todos aquellos que tratamos información personal de terceros debemos avanzar en fortalecer las capacidades para cumplir la Ley Federal de Protección de Datos Personales, y con esta obra se pretende coadyuvar al logro de este objetivo.

Comité editorial del INAI.

PRÓLOGO

Hace unos meses cuando el INAI me invitó a coordinar la Ley comentada que el lector tiene en sus manos, me pareció un reto desafiante por dos motivos. El primero de ellos es porque soy un ferviente convencido que las leyes comentadas son obras que pueden implicar mucho esfuerzo y que de un plumazo el legislador termina destruyéndolas. El segundo motivo era porque tenía que buscar un conjunto de profesionales que estuvieran en el campo de batalla enfrentando las problemáticas cotidianas que la protección de datos arroja y hacer que se entusiasmaran con escribir, bajo un formato más elaborado, estudios que comentaran la Ley pero que dejaran un poco más de "pozo" conceptual al trabajo que la mera cita legal. Es así como se plantea esta obra. El lector no encontrará comentarios pormenorizados de cada artículo, por el contrario, hemos desarrollado, todos los que participamos en esta obra, estudios que analizan el contenido normativo con una visión más amplia y tendiente a generar aportaciones en el tratamiento de datos personales. Así fuimos integrando, a partir de cada capítulo de la Ley, diversos trabajos que comentan, perfilan, enfocan y sugieren mayores y más ambiciosos enfoques que sólo el quehacer legislativo.

En ese sentido me gustaría perfilar también este prólogo, pues al hablar de protección de datos es necesario hacerlo también del derecho a la vida privada y, en un mundo profundamente individualista, parecería una tarea sencilla pero no lo es. A pesar de que la modernidad ha ofrecido al individuo una consolidación de su esfera particular, también (sobre todo en los últimos años con la aparición de las nuevas tecnologías) ha vuelto exponencial la fragilidad de un entorno reservado, en principio, sólo a la persona.

La vida privada no es una asignación novedosa o contemporánea. Lo novedoso es su fragilidad ante los desafíos tecnológicos que se desarrollan día a día. Desde muchos siglos atrás encontramos referencias a lo privado como oposición a lo público. Existe una fuerte tradición sobre la contraposición entre lo privado y lo público, pues ya desde el mundo antiguo se habla de lo privado como un paso fundamental para acceder a lo público.

Hoy en día la vida privada se identifica con el derecho a estar solo, el derecho a la intimidad, el derecho a la privacidad, el derecho a no ser molestado e incluso se limita a la autodeterminación informativa, pero ello es erróneo toda

vez que cada una de estas nomenclaturas tiene alcances y consecuencias diversas o bien forman parte de un género más amplio que llamaremos: derecho a la vida privada.

Una primera aproximación a la vida privada nos lleva a afirmar que representa la esencia del individuo en cuanto a ser humano, es decir, la vida privada representa la propia individualidad entendiendo ésta como el conjunto de pensamientos, sentimientos, expresiones y manifestaciones sobre sí mismo o una esfera reducida de expansión de dicha individualidad.

Desde la lengua castellana encontramos referencias a lo privado y a la privacidad como ámbitos diferenciados. En ese sentido la Real Academia de la Lengua (RAE) refiere que por privado (a) entenderemos un adjetivo *"*que se ejecuta a vista de pocos, familiar y domésticamente, sin formalidad ni ceremonia alguna*"*, mientras que por privacidad entendemos *"*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*"*, en ese sentido refiere la RAE que la expresión "en privado" significará "a solas o en presencia de pocos, sin testigos".

La vida privada está guiada por el valor supremo de la libertad, que se manifiesta, en un primer momento, a partir de la libertad de conciencia donde el individuo tiene libertad de pensar, sentir, expresar y manifestar sus opiniones. En un segundo momento, la libertad ayuda a trazar el plan de vida para actuar como se quiera, siempre mirando a las consecuencias de los actos y, finalmente, para poder reunirse con quien le guste y plazca, sin ánimo de dañar a otros.[1]

La vida privada "se asimila a la vida retirada o anónima, a la vida interior..."[2] en ese sentido no es casual que la doctrina norteamericana se refiriera a ella como "la potestad del titular a vivir solo y a no ser molestado, que permite al individuo decidir soberanamente sobre sobre su independencia personal".[3]

La vida privada es aquella que no está dedicada a una actividad pública[4] y que por ende es intrascendente y no tiene impacto en la sociedad de manera directa,[5] donde, en principio, los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia ni les afecta. Se encuentra protegida desde diversas perspectivas dentro de los

1 Sánchez, J. (2012). *Voluntad Anticipada*. México. Porrúa, pp.68 y 69.
2 Carrillo, M. (2003). *El derecho a no ser molestado*. Navarra Thomson-Aranzadi, p. 44.
3 Ídem.
4 Habermas, J. (2004). *Historia y crítica de la opinión pública*. Barcelona, GILI, p.50.
5 Carrillo, M. (2003). *El derecho a no ser molestado*. Navarra. Thomson Aranzadi, p. 44. Refiere el autor que: "…es la potestad del titular a vivir sólo y a no ser molestado, que permite al individuo decidir soberanamente sobre su independencia personal".

distintos marcos constitucionales,[6] pero la más importante es donde se protege de cara a los posibles abusos que puedan existir por parte del poder o de otros particulares.[7]

Hoy en día, cuando nos referimos a la vida privada en los marcos constitucionales también hablamos de la autodeterminación informativa como un derecho constitucional inserto en la vida privada y que, sin lugar a dudas, con el advenimiento de las nuevas tecnologías completa el cuadro de protección del derecho que referimos.

De igual manera los tribunales, tanto nacionales como internacionales, se han volcado a establecer el contenido esencial del derecho a la vida privada. En ese sentido el máximo tribunal mexicano lo ha referido como aquel "que no constituye vida pública"[8] como "el ámbito reservado frente a la acción y al conocimiento de los demás",[9] "lo que se desea compartir únicamente con aquellos que uno elige",[10] "las actividades que las personas no desempeñan con el carácter de servidores públicos".[11] Desde este punto de vista establecido por la Corte mexicana, "las personas tienen derecho a gozar de un ámbito de proyección de su existencia que quede reservado de la invasión y la mirada de los demás, que les concierna sólo a ellos y les provea de condiciones adecuadas para el despliegue de su individualidad —para el desarrollo de su autonomía y libertad".[12]

A la par de la Corte mexicana, la Corte Interamericana de Derechos Humanos se ha manifestado en torno a este derecho que llamamos "vida privada" y en ese sentido dicho tribunal ha referido que "la protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo…"[13] en donde él mismo tendrá "la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales".[14]

Para la Corte Interamericana, la vida privada no sólo se proyecta desde una perspectiva de interioridad del individuo, por el contrario, refiere que la misma "…engloba aspectos de identidad física y social, incluyendo el derecho

6 En el caso mexicano protegido en el artículo 16 constitucional.
7 Carrillo, *op. cit*. P. 44
8 Semanario Judicial de la Federación. (2009, diciembre). *Derecho a la vida Privada. Su contenido general y la importancia de no descontextualizar las referencias de la misma*. Novena época. Registro 165823. Primera Sala. Tesis aislada. Tomo XXX, p. 277.
9 Ídem.
10 Ídem.
11 Ídem.
12 Ídem.
13 Corte Interamericana de Derechos Humanos. *Caso Artavia Murillo y otros (fertilización in vitro) vs Costa Rica*, párrafo 143.
14 Ídem.

a la autonomía personal y desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior".[15]

Dicho derecho a la vida privada constituye, para el Tribunal Interamericano, un derecho de capital importancia para el desarrollo personal, en ese sentido, es necesario que todo Estado lo proteja y lo haga efectivo pues ello es decisivo *"…*para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona".[16] Ello permite configurar dos elementos muy relevantes de la vida privada, por un lado "la forma en la que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás y como condición indispensable para el libre desarrollo de la personalidad".[17]

El derecho a la vida privada ha sido enunciado y, en ocasiones, confundido con el concepto de "privacidad" o bien con el derecho a la intimidad. Esta confusión no es gratuita y tiene una explicación. Si bien es cierto que la noción de vida privada tiene un "pozo" histórico importante, también es cierto que su conceptualización como derecho data apenas de finales del siglo XIX con el famoso ensayo de Warren y Brandeis de 1890 llamado *The right to privacy*[18] en el cual, en realidad, se entendía por "privacidad" a una noción de lo que hoy conocemos como "intimidad" pues el carácter de lo privado radicaba en una limitante para la autoridad o para terceros como puede ser la prensa, de no intervenir en la esfera más íntima de la persona.

De igual manera, es imperante señalar que hoy el concepto de vida privada adquiere nuevos derroteros en función a los cambios vertiginosos de la tecnología de nuestro tiempo. En ese sentido, las tecnologías de la información han propuesto nuevos desafíos a los alcances del derecho a la vida privada. Expresiones como *big data, cloud, e-learning, cyberacoso, cyberdelitos* etc. están suponiendo una reconfiguración del concepto de vida privada.

La vida privada se excluye del principio de máxima publicidad, principio rector de la política de transparencia y del derecho de acceso a la información contenido en las constituciones que prevén dicho derecho. Una de las típicas excepciones al principio de máxima publicidad es el ámbito de la confidencialidad, es decir, el derecho que tiene toda persona para mantener en reserva su información sin que nadie pueda utilizarla sin su consentimiento.[19]

---

15 Ídem.
16 Ídem.
17 Ídem.
18 Carrillo, M. *op. cit.* p.36.
19 Desantes-Guanter, J. (2004). *Derecho a la Información*. Valencia. Fundación COSO, p. 230. El autor se refiere a que "…en ningún caso se puede penetrar en la intimidad de las personas contra su voluntad…".

Como referíamos anteriormente, dentro de la esfera que denominamos "vida privada" se desarrolla otro derecho que ha cobrado fuerza en materia de autodeterminación informativa que es el llamado "derecho a la intimidad". Es aquel centrado en lo más profundo de la persona, en donde se desarrollan sus pensamientos, aficiones, preferencias sexuales y políticas, creencias religiosas y demás situaciones que sólo le pertenecen a la persona y que puede compartirlas con un número muy reducido de personas.[20] El derecho a la intimidad tiene una fuerte relación con la autodeterminación informativa, pues dentro de ella, cuando hablamos de datos sensibles, nos referiremos a aquellos vinculados a esta esfera íntima de la persona.

Tanto el derecho a la vida privada como el derecho a la intimidad adquieren relevancia en la autodeterminación informativa al constituir el núcleo central de la administración de la información personal que sólo por voluntad es susceptible de ser compartida. Normalmente, en los marcos constitucionales democráticos, estos derechos están en franca oposición con la publicidad de la información, la cual siempre deberá velar por la protección de ambos y no sólo ello, cuando llegan a colisionar, permitirá que éstos, en la mayoría de las ocasiones, triunfen sobre la publicidad.

Existen otros derechos que pueden violentarse con la invasión a la vida privada y a la intimidad como son, entre otros, el derecho al honor y el derecho a la propia imagen, los cuales, en conjunto con la vida privada, formarán lo que la tradición civilista ha denominado los derechos de la personalidad, y que han cobrado especial preponderancia cuando hay tratamientos inadecuados de datos personales.[21] Es por ello que es de capital importancia que los retos fundamentales del derecho a la privacidad hoy en día estén enfocados en proteger a este conjunto de derechos.

En ese sentido, desde mediados del siglo pasado surgió, en varias partes del mundo, la preocupación de proteger los datos personales de los individuos como una forma de proteger su vida privada. Su indebida difusión supone un ejercicio de invasión a la vida privada sin precedentes. Dicha protección fue ganando terreno hasta alcanzar los planos constitucionales, siendo ello,

---

[20] El derecho a la intimidad significará "… la absoluta soledad, en donde la persona vive íntegra y absolutamente su vida auténtica." Ibídem., p. 229.

[21] En ese sentido la Suprema Corte de Justicia de la Nación en su tesis *Derecho a la vida privada. Su contenido general y la importancia de no descontextualizar las referencias a la misma* ha referido un catálogo enunciativo de derechos conexos con la vida privada como lo son: "… el derecho de poder tomar libremente ciertas decisiones atinentes al propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, la protección contra el espionaje, la protección contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular." Semanario Judicial de la Federación. (2009, diciembre). Novena época. Tomo XXX, p. 227.

un paso muy importante para agregarlo como un apartado adicional de la configuración de la vida privada.

Es así como la vida privada amplía sus dimensiones. Ya no se trata de protegerla de los abusos de la autoridad o de los medios tradicionales por la difusión de información no propia para lo público, ahora se trata de protegerla desde un ámbito diferente, que no es real sino virtual pero que produce efectos, quizá, más devastadores.

Estos efectos (todavía no vistos con total claridad) están generando, a nivel mundial, una preocupación grande sobre los alcances de la vida privada en un mundo virtual. Basta mencionar algunos esfuerzos en el continente americano como la Declaración de Lima (2013), de Barranquilla (2013), de Buenos Aires (2013), de Santiago (2013), de la Plata (2013) y de Riobamba (2014) en donde la preocupación se extiende a la protección de la vida privada de los menores, la cual está siendo de las más vulneradas por el acceso que tienen a las nuevas tecnologías.

Con todo lo anterior podemos destacar que el derecho a la vida privada incluye:

a) El derecho a no ser molestado
b) El derecho a estar solo
c) El derecho a la confidencialidad
d) El derecho a la protección de datos
e) El derecho a la autodeterminación informativa
f) El derecho al olvido digital
g) El derecho a la intimidad

La confidencialidad de la vida privada y la autodeterminación informativa

De manera complementaria hay que decir que la vida privada tiene en la confidencialidad a su principal atributo.[22] En el caso de la información que guarda especial relación con la vida privada o íntima de las personas, la limitación a la publicidad de la misma se presenta como natural al manejo de aquella. En este caso, es preciso que dicha información sea clasificada con tal naturaleza de confidencial, por tratarse de un bien jurídico que, en ponderación con lo público, no participara de dicho elemento. La información confidencial no es, por esencia, información pública y en nada abona a lo público. La confidencialidad conlleva un no hacer (la divulgación) y un hacer (el manejo sigiloso de la información).

[22] Según el *Diccionario de la Real Academia de la Lengua Española*, la confidencia obedece a "la acción de confiar reservada o secretamente algo a una persona de confianza". En ese sentido el carácter de guardar la confidencialidad corresponderá a aquel al que se le entregó la información.

A pesar de lo anterior, puede darse el caso de que a partir de la información confidencial obtengamos datos estadísticos que nos sirvan para la decisión pública, pero dicho uso estará supeditado a un proceso de disociación[23] en donde la vida privada o íntima no sea menoscabada.

La información confidencial no podrá ser revelada, salvo que medie consentimiento del particular que la proporcionó. Es más, para efectos de este tipo de información, el poder público deberá, en todo momento, asumir una serie de mecanismos de seguridad para el debido resguardo y protección, siendo que, y desde su obtención, se deberá informar al titular del uso qué se hará con la información, para qué fines se obtiene, si será susceptible de divulgación y cómo se efectuará su almacenamiento.[24] Lo mismo sucede en el ámbito privado, donde la información entregada con el sello de "confidencial" asumirá un tratamiento específico en los llamados responsables.

En el caso del poder público, la protección de información personal por parte del Estado debe ser garantizada, más que como una limitación del derecho de acceso a la información, como un derecho fundamental derivado del derecho a la vida privada a partir de lo que se denomina autodeterminación informativa. Dicha protección deberá cubrir todas las previsiones de seguridad de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).[25] De igual manera, en el ámbito privado, la garantía de cuidado de la información estará llamada a respetar, no sólo la vida privada, la intimidad y la autodeterminación informativa, sino también los derechos al honor y en ocasiones la propia imagen.

Esta llamada autodeterminación informativa garantizará al ciudadano una serie de derechos que son conocidos por su acrónimo como los derechos ARCO es decir a) acceso, b) rectificación, c) cancelación y d) oposición. Acompañando a estos derechos estará la institucionalización de medidas de seguridad en tres vías para el aseguramiento de un tratamiento adecuado, que constituirán obligaciones de todos los sujetos obligados. Así,

[23] Cabe recordar que en la Ley Federal de Datos Personales en Posesión de los Particulares la disociación se encuentra referida en el artículo 3º Fracción VIII en donde se refiere como un mecanismo aceptable para la divulgación de datos estadísticos que se nutren, en primer lugar, de datos de la vida íntima o privada de las personas. En ese sentido, dicho proceso de disociación involucrará un desgajamiento entre la información que le da origen y el dato que nos interesa publicar y en donde sería imposible identificar a las personas que nutren en su conjunto el dato estadístico.

[24] Villanueva, E. (2003). *Derecho de acceso a la información pública en Latinoamérica*. México. IIJ-UNAM, p. 74. De esta manera, se encuentra contemplado tanto en la Ley Federal de Acceso a la Información Pública como en la Ley General de Datos Personales en Posesión de los Sujetos Obligados.

[25] Ídem. En el ordenamiento jurídico mexicano, la defensa a la vida privada encontrará, tanto en el artículo 6 como en el 16 de la Constitución, manifestaciones claras de protección, es por ello que tanto la Ley Federal de Transparencia y Acceso a la Información como la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados reforzarán el carácter confidencial de la información que goza de esta característica.

i) habrá medidas de seguridad técnicas destinadas a la protección y resguardo seguro de la información, ii) las medidas físicas que asegurarán el tratamiento de la información contenida en soportes tradicionales y iii) las medidas de seguridad administrativas, las cuales estarán destinadas a proponer mecanismos o procedimientos que irradien a todo el enramado organizacional para el debido cuidado de la información de carácter personal. Ello implicará, no sólo un deber de cuidado, sino una responsabilidad que, en el caso de ser incumplida, implicará una sanción para el funcionario, tratándose de información otorgada a los órganos del Estado, o bien para los responsables, en el caso de entidades de naturaleza privada.

La autodeterminación informativa y la protección de datos tienen como objeto primordial: la protección de la información. Esta información tiene como rasgos distintivos que es susceptible de ser apropiada desde su origen y que pertenece originariamente a su autor, siendo que esta información está compuesta de datos y, como sabemos, un conjunto de datos constituye información.

En ese sentido podemos afirmar que el derecho a la autodeterminación informativa supone un ejercicio de libertad del individuo para proporcionar sus datos o la información respecto a sí mismo, a su entorno, a su domicilio, posesiones y afectos a un tercero. Este ejercicio de libertad se mueve a partir del conocimiento que la persona tenga sobre lo que ocurrirá con la entrega de sus datos e información, conozca los alcances y otorgue su pleno consentimiento para que se lleve a cabo su manejo. De lo contrario, no podemos hablar propiamente de autodeterminación informativa.

A la par de la autodeterminación informativa se configura la protección de datos personales y se propone como una garantía que otorga el poder público para que tenga un respaldo lo suficientemente fuerte y que involucre al poder del Estado para evitar abusos, delitos o cualquier especie de menoscabo de dicha autodeterminación. No es gratuito que hoy se hable de un derecho *a* y de un derecho *de* la protección de datos.

Tanto la autodeterminación informativa como la protección de datos han cobrado una fuerza muy relevante en los últimos años (como se ha dicho anteriormente) por el desarrollo de nuevas plataformas tecnológicas, las cuales han permitido el tráfico de datos de manera exponencial y en ocasiones, sin ninguna protección. Hoy hablamos de "poder informático"[26] como aquel que dota a determinados agentes a "…acumular informaciones sobre cada persona en

[26] Delpiazzo, C. (2012). "Relaciones entre privacidad y transparencia". En Tenorio C. y Guillermo, A. *Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares*. México. Porrúa, p. 7.

cantidad ilimitada, de memorizarla, usarla, transferirla como una mercancía..."[27] y almacenarla para su posterior uso de manera indiscriminada y, en muchas ocasiones, sin el consentimiento del titular como es el caso de *datamining* (búsqueda de información sensible escondida dentro de las bases de datos).[28]

La fuerza que han adquirido estos dos derechos ha venido de la mano del crecimiento de las mencionadas tecnologías. Es por ello que el Estado, a través de su marco normativo, está llamado a tratar de seguir, de manera más eficaz, el desenvolvimiento de estas nuevas tecnologías, previendo, por un lado, a través de la legislación y resolviendo, por otro, mediante el trabajo intenso de los tribunales, los asuntos que plantean estos nuevos entornos digitales respecto al dinamismo en el flujo de la información para ofrecer al ciudadano una mejor y mayor protección del manejo de sus datos.

La obra que el lector tiene en sus manos explorará todos los derroteros referidos con anterioridad. No me resta sino agradecer a cada uno de los autores de esta obra que con esfuerzo, dedicación, paciencia y laboriosidad construyeron los apartados que constituyen este trabajo. En ese sentido, basta decir gracias a Alfredo Reyes, Cynthia Solís, Héctor Guzmán, Nuhad Ponce, Wilma Arellano, Luis Ricardo Sánchez, Andrea Mendoza, Carlos Requena y Miguel Ángel Flores y, desde luego, a los comisionados del INAI por la confianza para llevar a cabo este trabajo.

Dr. Guillermo A. Tenorio Cueto.
Ciudad de México, 15 de enero 2019.

Referencias

Carrillo, M. (2003). *El derecho a no ser molestado*. Navarra. Thomson-Aranzadi.

Corte Interamericana de Derechos Humanos. *Caso Artavia Murillo y otros (fertilización in vitro) vs. Costa Rica*. Párrafo 143.

[27] Ibídem, p.8
[28] Ídem.

Delpiazzo, C. (2012). “Relaciones entre privacidad y transparencia”. En Tenorio C. y Guillermo, A. *Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares*. México. Porrúa.

Desantes-Guanter, J. (2004). *Derecho a la Información*. Valencia. Fundación COSO.

Habermas, J. (2004). *Historia y crítica de la opinión pública*. Barcelona. GILI.

Lucas. P. (2008). “El derecho a la autodeterminación informativa y la protección de datos personales*”. Cuadernos de derecho.* Azpilcueta. España. No. 20.

Orrego, C. (2013). Una aproximación al contenido constitucional del derecho de autodeterminación informativa. *Anuario de derecho constitucional latinoamericano*. Año XIX. Bogotá, p. 326.

Riande, N. (2017, julio). El derecho a la autodeterminación informativa, praxis de la justicia administrativa. *Revista del Tribunal Federal de Justicia Administrativa*. No. 21, p. 11.

Riande, N. (2017). El derecho a la autodeterminación informativa. *Praxis de la justicia administrativa*. Tribunal Federal de Justicia Administrativa, No. 21, p. 11.

Sánchez, J. (2012). *Voluntad Anticipada*. México Porrúa.

Suprema Corte de Justicia de la Nación. (2009, diciembre). Derecho a la vida privada. Su contenido general y la importancia de no descontextualizar las referencias a la misma. *Semanario Judicial de la Federación*. Novena época. Tomo XXX, p. 227.

Tellez, J. (2013). Lex Cloud computing. Estudio jurídico del cómputo en la nube en México. México IIJ-UNAM, p.134.

Villanueva, E. (2003). Derecho de acceso a la información pública en Latinoamérica. México. IIJ-UNAM

SEMBLANZA DE LOS AUTORES

Guillermo A. Tenorio Cueto

Es licenciado y doctor en derecho por la Universidad Panamericana. Actualmente ocupa el cargo de director del posgrado de la Escuela de Gobierno y Economía de esa misma Universidad. Es copresidente de la fundación Cooperación Iberoamericana de Transparencia y Acceso a la Información (CITYAI) y consultor independiente en materia de protección de datos desde hace 10 años. Fue director general del Centro de Estudios Superiores en Materia de Justicia Administrativa y Fiscal del Tribunal Federal de Justicia Administrativa en México, catedrático de derecho a la información en la Universidad Panamericana y profesor de posgrado de materias como Derecho a la vida privada, Protección de datos personales y Transparencia y acceso a la información en diversas casas de estudio de nuestro país. Es autor, coordinador y editor de 15 libros en libertades informativas y de más de 40 artículos sobre derecho a la información, publicados en diversas revistas jurídicas especializadas. Además, es miembro del Sistema Nacional de Investigadores de México. Ha dictado conferencias sobre derecho a la información y protección de datos personales en diversos foros nacionales e internacionales y es profesor visitante en varias universidades de Iberoamérica. Ha participado en diversos medios de comunicación con temas de derecho de la información y protección de datos personales. Fue, durante cinco años, director de contenidos y conductor del programa de televisión: *Ante la ley* en el *Canal Judicial en México*. Fue designado, por mayoría absoluta, en la LXII legislatura como consejero honorario de transparencia y acceso a la información de la Cámara de Diputados del H. Congreso de la Unión de México.

Alfredo Reyes Krafft

Es doctor en derecho, con la mención *Cum Laude*, por la Universidad Panamericana. Tiene un posgrado en dirección de empresas (D1) en el Instituto Panamericano de Alta Dirección de Empresa (IPADE) y una especialidad en contratos y daños por la Universidad de Salamanca. Ha sido contralor jurídico del Banco del Atlántico, miembro del comité consultivo de la organización sin fines de lucro NIC México y de *Innovation Concepts* y *Regulation*, director en BBVA y presidente de la Asociación Mexicana de Internet (AMIPCI).

Actualmente es socio director en Lex Inf IT Legal Advisory y *Board Member* Director de GLEI. Obtuvo el *Secure Award* 2009, así como el reconocimiento que otorga la AMIPCI a la trayectoria en internet (2009 y 2012) y la distinción Abogado Digital 2018 por *Foro Jurídico*. También fue coordinador nacional del ISO/IEC JTC 1SC 27/WG 2 *Cryptography and Security Mechanisms*.

El doctor Reyes es el primer mexicano reconocido con la certificación *Certified Data Privacy Professional*. También es experto técnico por la Entidad Mexicana de Acreditación (EMA) organismos de certificación y protección de datos personales en posesión de los particulares. Ha trabajado como docente en varias instituciones universitarias, entre las que destacan la Universidad Panamericana (UP), la UNAM, el ITESM, el IPN, el Infotec del Conacyt y la Universidad de Salamanca en España. Además, es autor del libro *La firma electrónica y las entidades de certificación* que la editorial Porrúa publicó en 2003 y 2005. Con relación en la protección de datos, es coautor de los libros *Protección de Datos Personales. La voz de los actores* de Tiro Corto Editores, publicado en 2010, *Los Datos Personales en México. Perspectivas y retos de su manejo en posesión de particulares* por Porrúa y la UP en 2012, *La Protección de los Datos Personales en México* por Tirant Lo Blanch, 2013. Asimismo, es autor de las voces: *Legislación Mexicana en materia de Protección de Datos Personales y Autorregulación* y *Sellos de Confianza en la Obra Jurídica Enciclopédica* (Volumen derecho informático e informática jurídica) publicado por Porrúa y el Centro de Investigación e Informática Jurídica de la Escuela Libre de Derecho en 2012.

Cynthia Solís Arredondo

Es licenciada en derecho por la UNAM y doctora en derecho privado y ciencias criminales por la Universidad de Paris Saclay. Tiene diversos estudios de posgrado en las universidades de Paris I Panthéon Sorbonne, Paris Sud XI, la UP y en el Colegio de México. Se ha especializado en las áreas de propiedad intelectual, cibercriminalidad, *fashion law* y protección de datos personales. Es catedrática de distintas universidades e instituciones educativas nacionales e internacionales como el IPN, CESNAV y el INACIPE. Es experta certificada en materia de protección de datos personales por NYCE y socia fundadora de la firma Lex Inf IT Legal Advisory.

Héctor Guzmán Rodríguez

Es licenciado en derecho por la Universidad Iberoamericana, donde también estudió un diplomado en derecho corporativo. Tiene un *máster* en derecho de la Unión Europea por la Universidad Complutense de Madrid y es licenciado en derecho por la Universidad de Zaragoza. Se desempeña como miembro de la *International Association of Privacy Professionals* (IAPP), la Academia

Mexicana de Derecho Informático (AMDI), el Colegio de Abogados de Madrid (ICAM), la Asociación Profesional Española de Privacidad (APEP) y colabora con el Observatorio Iberoamericano de Protección de Datos (Oiprodat). Como coautor, ganó los premios Protección de Datos Personales de Investigación (Accésit- 2014) otorgado por la Agencia Española de Protección de Datos por la obra *Protección de datos y habeas data: una visión desde Iberoamérica* y el Premio Investigación en Protección de Datos (2018) otorgado por la Agencia Vasca de Protección de Datos por el libro *Hacia una efectiva protección de los datos en Iberoamérica*. *Declaraciones de la iniciativa del Observatorio Iberoamericano de Protección de Datos*.

Wilma Arellano Toledo

Es doctora por la Universidad Complutense de Madrid con especialidad en derecho de la información y derecho de las TIC, con calificación de *Sobresaliente Cum Laude*. Ha sido investigadora invitada en el Instituto Complutense de Estudios Jurídicos Críticos (ICEJC) y en el Centro de Estudios Políticos y Constitucionales (CEPC) del Ministerio de la Presidencia de España. Actualmente es investigadora en la Universidad San Pablo (CEU) de Madrid en el departamento de derecho público. Es miembro del grupo de investigación Social Impact of Artificial Intelligence and Robotics (Simpair) de la red Derechotics y del grupo de investigación del proyecto *El avance del Gobierno Abierto. Régimen jurídico constitucional de la implantación de la transparencia, datos abiertos y participación especialmente a través de TIC y E-Gov*, financiado por el Ministerio de Economía y Competitividad de España. Es miembro del comité científico y organizador del XV Foro Internacional de Ética y Derecho de la Información (FIEDI antes CIEDI) en el marco de la Conferencia de la International Association For Media and Communication Research (IAMCR). Publicó el libro *Política y Derecho de las telecomunicaciones en Europa, Norteamérica y México* (2009) y coordinó los libros colectivos *El iusinformativismo en España y México y La Sociedad de la Información en Iberoamérica. Estudio multidisciplinar* (2013), obra colectiva en la que participan 28 autores de México, España, Chile, Argentina y otros países.

Asimismo, ha publicado alrededor de 30 capítulos en libros de editoriales de prestigio, aproximadamente 21 artículos en revistas arbitradas e indexadas sobre derecho y las TIC, con especial atención a los aspectos relativos a tecnologías de la información y la comunicación, telecomunicaciones, privacidad y protección de datos personales en el entorno TIC y derecho a la información. Ha participado con ponencias, conferencias magistrales y debates en más de 40 eventos académicos en España, México, Chile, Argentina e Inglaterra y ha sido miembro de los comités científicos de ocho congresos internacionales. Es miembro de la red *Derechotics* de España, de la International Association For Media and Communication Research en su *section law*, de la Asociación

Mexicana de Investigadores en Comunicación y de la Asociación Mexicana de Derecho a la Información, de la que también formó parte del comité directivo en el periodo 2015-2017.

Luis Ricardo Sánchez Hernández

Es maestro en derecho de las tecnologías de información y comunicación (MDTIC) con estudios especializados en protección de datos digitales en el Centro de Investigación e Innovación en las Tecnologías de Información y Comunicación (Infotec) del Conacyt. Es licenciado en derecho por la Facultad de Derecho de la Universidad Autónoma del Estado de México, profesor en línea y presencial en la maestría en derecho de las tecnologías de la información y comunicación (MDTIC) del Infotec, así como de licenciatura y maestría en otras universidades. Además, se desempeña como titular de la Unidad de Planeación y Transparencia de la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de México y Municipios, director de protección de datos personales del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (Infoem), secretario de actas del Comité de Registro de Testigos Sociales del Estado de México, jefe del departamento de lo contencioso del Órgano Superior de Fiscalización del Estado de México.

Olivia Andrea Mendoza Enríquez

Es licenciada en derecho, maestra en derecho con especialidad en derecho económico y doctora en derecho con distinción *Ad Honorem* por la Benemérita Universidad Autónoma de Puebla, especialista en derechos humanos por la Universidad Castilla-La Macha (UCLM) en España, profesora investigadora titular de tiempo completo del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, (Infotec) del Conacyt, miembro del Sistema Nacional de Investigadores, nivel I, coordinadora académica y miembro del núcleo académico básico de la maestría en derecho y TIC, coordinadora académica de la maestría en regulación y competencia económica de las telecomunicaciones impartida a servidores públicos del Instituto Federal de Telecomunicaciones IFT. Su línea de investigación es regulación y tecnología, particularmente relacionada con el derecho a la protección de datos personales.

La doctora ha sido conferencista nacional e internacional y autora de diversos productos académicos en dichas temáticas y colaboradora en el Observatorio Iberoamericano de Datos Personales. Por su aportación a la cultura democrática, ganó el Premio Municipal de la Juventud en su edición 2013 que otorga el H. Ayuntamiento de Puebla. Fue profesora invitada de la División de Educación Continua de la Facultad de Derecho la UNAM. Se

ha destacado como docente del diplomado de protección de datos personales de la Escuela Libre de Derecho, del diplomado de privacidad, regulación y gobernanza de datos del Centro de Investigación y Docencia Económicas (CIDE), de la Universidad Iberoamericana campus Santa Fe, del Máster en *Legaltech* y gestión digital de la abogacía de la Universidad de Salamanca (USAL), España. Fue capacitadora en temas de protección de datos personales, transparencia y acceso a la información en el INAI. Fue participante del sector académico para la conformación de la Estrategia Nacional de Ciberseguridad (ENCS) para México, desarrolladora temática del Aula Iberoamericana de Protección de Datos Personales, miembro del grupo Iniciativa del Foro Mundial de Gobernanza en Internet, coordinadora e instructora del curso Protección de Datos Personales, impartido a través de la plataforma México X de *Televisión Educativa de México* y miembro del Consejo Consultivo de la Federación Iberoamericana de Asociaciones de Derecho Informático (FIADI).

Miguel Ángel Flores Guerrero

Es socio fundador y CEO de la firma Seprodat y especialista en protección de datos personales. Desde 2010 ha asesorado y capacitado a prestigiadas marcas en los sectores de seguros, financiero, automotriz, educativo, salud privada, químico farmacéutico, turístico y restaurantero en sus procesos de adaptación a la legislación en la materia. De 2004 a 2010 fue representante de la Asociación Mexicana de Instituciones de Seguros (AMIS) como parte del comité encargado de la elaboración, discusión y redacción de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Ha brindado conferencias y cursos en diversos foros como la Asociación Mexicana de Contadores Públicos (AMCP), la Asociación Internacional para la Protección de la Propiedad Intelectual (AMPPI), la Secretaría de Economía, el Instituto Tecnológico Autónomo de México (ITAM), el Instituto Sonorense de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (ISTAI) y el Instituto Tecnológico Superior de Puerto Peñasco, Sonora. Ha participado como invitado en programas de radio y televisión, como asesor en temas selectos de privacidad.

Nuhad Ponce Kuri

Es socia fundadora del despacho Ponce Kuri, S.C., directora del área de Protección de Datos Personales, Derecho Corporativo y Tecnologías de la Información y Comunicación. Es licenciada en derecho, egresada de la Universidad Panamericana, institución donde cursó la maestría en derecho de la empresa, titulada con mención honorífica. Está certificada por Normatividad y Certificación Electrónica, S.C. (NYCE) como profesional certificado en protección de datos personales, nivel senior. Es miembro de la International Association of Privacy Professionals (IAPP). Ha tomado diversos diplomados, especialidades y

cursos en contratos y negocios mercantiles, protección de datos personales y seguridad de la información, así como derecho de la propiedad intelectual. Es miembro del Consejo Directivo Nacional de la Asociación Nacional de Abogados de Empresa, Colegio de Abogados, A.C. (Anade) donde ha desempeñado diversos cargos. Actualmente forma parte de su consejo consultivo. Del año 2010 a la fecha, ha estado certificada como abogado de empresa por dicho colegio. Es miembro del consejo de la Asociación Jurídica Mexicano Libanesa, Al Muhami, A.C., catedrática en diversas universidades a nivel licenciatura y postgrado, conferencista en foros y congresos. Ha escrito múltiples artículos relacionados con el derecho corporativo, la protección de datos personales y seguridad de la información, entre otros temas afines, que han sido publicados en revistas especializadas nacionales e internacionales.

Carlos Requena Ochoa

Es penalista, socio del despacho Requena Abogados, S.C., experto en responsabilidad penal de empresa y *compliance* penal, profesor de derecho penal a nivel licenciatura y maestría en la Universidad Panamericana (UP), articulista de la columna “Derecho Reservado” en *El Semanario* y en *Red Forbes*, autor de los libros *Compliance Legal, una Tendencia Regulatoria Mundial* y *Fraude Procesal, Leyes Para Tu Bien* (ambos en Editorial Thomson Reuters Dofiscal) y *Human and Civil Rights* editado por la International Academy for Leadership de la Friedrich-Naumann-Stifftung en la República Federal Alemana. Además, ha sido conferencista y miembro de la International Barr Association (IBA). Cuenta con amplia experiencia en el manejo de crisis en contextos de litigio a favor de las empresas.

CAPÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. *La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.*

Artículo 2. *Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:*

I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y

II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Artículo 3. *Para los efectos de esta Ley, se entenderá por:*

I. Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley.

II. Bases de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable.

III. Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas.

Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.

IV. Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

V. Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

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

VII. Días: Días hábiles.

VIII. Disociación: 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.

IX. Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

X. Fuente de acceso público: Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación, de conformidad con lo señalado por el Reglamento de esta Ley.

XI. Instituto: Instituto Federal de Acceso a la Información y Protección de Datos, a que hace referencia la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

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

XIII. Reglamento: El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

XIV. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

XV. Secretaría: Secretaría de Economía.

XVI. Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

XVII. Titular: La persona física a quien corresponden los datos personales.

XVIII. Tratamiento: 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.

XIX. Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

Artículo 4. *Los principios y derechos previstos en esta Ley, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.*

Artículo 5. *A falta de disposición expresa en esta Ley, se aplicarán de manera supletoria las disposiciones del Código Federal de Procedimientos Civiles y de la Ley Federal de Procedimiento Administrativo.*

Para la substanciación de los procedimientos de protección de derechos, de verificación e imposición de sanciones se observarán las disposiciones contenidas en la Ley Federal de Procedimiento Administrativo.

COMENTARIO

Alfredo A. Reyes Krafft

Introducción

El derecho a la protección de datos de carácter personal es un derecho fundamental reconocido internacionalmente. Se trata de un derecho subjetivo, autónomo y de tercera generación que constituye un instrumento jurídico imprescindible para el desarrollo de la sociedad y que garantiza la privacidad y el derecho a la autodeterminación informativa de los individuos que la conforman. La ley que lo contiene fue publicada el 5 de julio del 2010 y explica las normas de orden público que son de carácter taxativo, y ello implica que los derechos que las mismas confieren a sus destinatarios son irrenunciables por voluntad de los particulares.

Este cuerpo normativo, en sus disposiciones generales, motivo del presente trabajo, indica con precisión los sujetos que se encuentran obligados al cumplimiento del mismo en virtud del tratamiento de datos personales que llevan a cabo, con dos excepciones particulares: la primera, derivada de un ordenamiento legal y la segunda, de una regla general, que contiene una excepción, misma que resulta aplicable siempre y cuando se cumplan con los requisitos correspondientes. A la par, en este apartado, el legislador dictó una serie de definiciones que permiten contar con un marco de referencia definido para la aplicación del ordenamiento legal que se analiza. Las definiciones que encontramos en este apartado son esenciales para la debida interpretación, que a lo largo del cuerpo normativo nos encontraremos.

En los dos últimos artículos del presente capítulo daremos cuenta que por un lado el legislador se refiere una regla general que se encuentra contenida en varios conjuntos normativos, relativa a los casos de excepción en los cuales es posible dejar de aplicar los principios y derechos establecidos en la misma

legislación y por otro el establecimiento de la regla general de supletoriedad aplicable al ordenamiento legal que nos ocupa.

Correlaciones

Artículos 6, 16 y 73 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM).

Artículos 1, 2, 3, 4, 5, 6, 7, 8, 49, 50, 51, 53, 54, 55 y del 113 al 139 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP).

Análisis de contenido

En México hemos tenido un importante desarrollo normativo en la materia, en una primera instancia con la entrada en vigor de las leyes de transparencia. El primer instrumento normativo en materia de protección de datos personales es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada el 11 de julio de 2002 en el *Diario Oficial de la Federación* que contempla apartados específicos en materia de protección de datos personales en el sector público. Años después se publicó una reforma al artículo 6º constitucional, el 20 de julio del 2007, que incorpora el término "datos personales" (en contexto con algunas reformas en materia de transparencia gubernamental):

> Artículo 6º
>
> ...El derecho a la información será garantizado por el Estado. Para el ejercicio del derecho de acceso a la información [...] en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
>
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

Otras disposiciones trascendentales fueron las reformas a los artículos 16 y 73 constitucionales en 2009, en los que se otorga reconocimiento a la protección de datos personales como un derecho fundamental y autónomo, y se faculta al Congreso de la Unión para legislar en la materia.

- En el artículo 16, segundo párrafo, se establece:

  > 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. (publicado el 1 de junio de 2009).

En el artículo 73 se establece:

> El Congreso tiene facultad: […] Para legislar en materia de protección de datos personales en posesión de particulares. (Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, publicado el 30 de abril de 2009).

Con la aprobación de dichas reformas se sentaron las bases para la expedición de una ley en la materia que regula el tratamiento de datos personales en posesión del sector privado, demanda latente desde 2000. Cabe notar que, en el ámbito estatal, los estados de Colima y Tlaxcala contaban ya con leyes de protección de datos para el sector público y privado. Jalisco en su código civil regulaba el derecho a la protección de datos personales en posesión de los entes privados. Las cuales fueron abrogadas o derogadas en términos del artículo quinto transitorio de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares:

- Quinto: En cumplimiento a lo dispuesto por el artículo tercero transitorio del Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el *Diario Oficial de la Federación* el 30 de abril de 2009, las disposiciones locales en materia de protección de datos personales en posesión de los particulares se abrogan, y se derogan las demás disposiciones que se opongan a la presente Ley.

Cuando se expidió la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en 2002, el Instituto previsto en ésta (el entonces IFAI) tenía la calidad de un organismo descentralizado de la administración pública federal, dependiente del presidente de la República. Su capacidad reguladora y de supervisión se limitaba a los órganos y dependencias del ámbito del Ejecutivo Federal.

Con la reforma al artículo 6 constitucional, el 7 de febrero de 2014, en materia de transparencia, se fortalecieron las atribuciones del organismo garante del derecho de acceso a la información y protección a los datos personales, otorgándole autonomía constitucional con la finalidad de generar un sistema de coordinación entre las entidades federativas y la Federación.

El 4 de mayo de 2015 se publicó la Ley General de Transparencia y Acceso a la Información Pública que transforma al antes IFAI en el Instituto Nacional de Transparencia y Acceso a la Información y Protección de Datos Personales (INAI).

En un segundo momento, en estas disposiciones generales, motivo de este trabajo, se determinan los sujetos que son regulados por el ordenamiento jurídico de referencia, para tal efecto, el legislador acude a la clasificación tradicional de persona física y de persona moral, con la particularidad de que sean de carácter privado.

Al respecto, consideramos oportuno remitirnos a la definición de derecho privado y de derecho público que nos proporciona el maestro Federico Jorge Gaxiola Moraila, donde indica que provienen del latín *privatium jus* y *publicum jus,* respectivamente, que significan "derecho concerniente a los particulares" y "derecho que atañe a las cuestiones públicas".[29]

Particularmente, define como derecho privado el conjunto de normas que regulan las relaciones jurídicas entre personas que se encuentran legalmente consideradas en una situación de igualdad, en virtud de que ninguna de ellas actúa, en dichas relaciones, investida de autoridad estatal.[30]

A continuación, con la expresión: "el tratamiento de datos personales" el legislador se refiere, de forma expresa, a dos conceptos fundamentales para la comprensión del ordenamiento legal que se analiza, mismos que por su importancia se da a la tarea de proporcionar una definición específica en el artículo 3 fracción XVIII, donde indica que se entiende por "tratamiento", a saber: "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".

En esta tesitura, el análisis de la expresión citada nos remite a la fracción V del dispositivo legal en cita, donde, puntualmente, nos proporciona una definición de "datos personales", al respecto, señala que se trata de "cualquier información concerniente a una persona física identificada o identificable".

Lo que antecede, para efectos de mejor proveer se suplementa con lo dispuesto en la fracción VIII del artículo 2 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, donde se dispone que "persona física identificable" es toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información. Por

[29] García, F. (2005). Derecho privado y derecho público, en *Diccionario Jurídico Mexicano del Instituto de Investigaciones Jurídicas*. México. Porrúa-UNAM, p. 1229.
[30] Ídem.

el contrario, no se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas.

Ahora bien, por lo que hace a la excepción que se desprende del inciso a), encontramos que la Ley para Regular las Sociedades de Información Crediticia de conformidad con lo indicado por su artículo 1, dicha ley tiene por objeto regular la constitución y operación de las sociedades de información crediticia. Para constituirse y operar como sociedad de información crediticia se requerirá la autorización del gobierno federal, misma que compete otorgar a la Secretaría de Hacienda y Crédito Público, oyendo la opinión del Banco de México y de la Comisión Nacional Bancaria y de Valores. Por su naturaleza, estas autorizaciones serán intransmisibles.

La prestación de servicios consistentes en la recopilación, manejo y entrega o envío de información relativa al historial crediticio de personas físicas y morales, así como de operaciones crediticias y otras de naturaleza análoga que éstas mantengan con entidades financieras, empresas comerciales o con una sociedad financiera de objeto múltiple (Sofom) no reguladas (ENR) sólo podrá llevarse a cabo por sociedades que obtengan la autorización antes mencionada.

Es de hacer notar que la excepción en comento es sólo para las sociedades de información crediticia y no para sus usuarios, quienes deben cumplir con lo dispuesto en la Ley de Protección de Datos Personales que les corresponda y además con la Ley de Sociedades de Información Crediticia y su normatividad secundaria.

Son usuarios de una sociedad de información crediticia quienes otorgan el crédito y se encargan de proporcionar la información sobre sus clientes y también consultan, de manera cotidiana, dicha información. Estos pueden ser:

- Entidades financieras: instituciones de crédito, organismos públicos cuya actividad principal sea el otorgamiento de créditos, fideicomisos de fomento económico constituidos por el gobierno federal, sociedades cooperativas de ahorro y préstamo, uniones de crédito, entidades de ahorro y crédito popular, instituciones de tecnología financiera y Sofomes.
- Empresas comerciales: aquellas empresas que realizan operaciones de crédito relacionadas con la venta de sus productos o prestación de servicios, los fideicomisos de fomento económico constituidos en cualquiera de los 32 estados de la República, así como la persona moral y el fideicomiso que adquieran o administren carteras crediticias.

Por otra parte, encontramos que el inciso b) del artículo en comento, refiere como excepción a 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.

Con lo anterior se establece una regla general que permite se lleve a cabo la recolección y almacenamiento de datos personales, sin embargo, lo somete a dos condiciones: la primera es que sea para uso exclusivamente personal y la segunda que sea sin fines de divulgación o utilización comercial.

Al respecto, consideramos que dicha regla general se encuentra plenamente justificada toda vez que en el eventual caso de que se lleven a cabo las acciones de recolección y almacenamiento de datos personales, las mismas no trascienden al ámbito jurídico en virtud del uso que se les dé y los fines que se persigan por la persona física correspondiente.

Con relación a este punto, el artículo 6 del Reglamento de la Ley especifica que cuando el tratamiento tenga como propósito cumplir con una obligación derivada de una relación jurídica, no se considerará para uso exclusivamente personal, en consecuencia, no caerá en el supuesto de excepción que hemos revisado.

Por último, encontramos que, no obstante, el contenido del dispositivo legal en cita se refiere de forma específica a las personas físicas y morales. El artículo 8 del Reglamento contempla la posibilidad de que grupos sin personalidad jurídica, es decir, personas integrantes de un grupo que actúen sin personalidad jurídica y que traten datos personales para finalidades específicas o propias del grupo se considerarán también responsables o encargados, según sea el caso.

Las disposiciones generales que comentamos no pueden eludir realizar un catálogo de definiciones que permitan precisar los conceptos que sirven de materia interpretativa de la ley. Así, el artículo 3 de la ley que hoy comentamos establece 15 fracciones que engloban los términos que el legislador consideró medulares para poder entender el cuerpo normativo. Así, la fracción I se refiere a una de las figuras más importantes contenidas en el ordenamiento legal objeto de estudio, el aviso de privacidad, mismo que es definido a través de diversos conceptos que a su vez son delimitados por el legislador tanto en el texto legal como el conjunto reglamentario correspondiente.

En primer término clarifica que el documento en cita es generado por “el responsable” del cual se ocupa la fracción XIV del mismo dispositivo legal y lo señala como: “Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales”.

A su vez, refiere que dicho documento es puesto a disposición del titular, cuya definición se encuentra contenida en la subsecuente fracción XVII que refiere al titular como: "La persona física a quien corresponden los datos personales" cuya referencia específica encontramos en la fracción V del mismo artículo.

Al respecto, establece que el tratamiento de los datos personales se hará de conformidad con el artículo 15 del mismo conjunto normativo, cuya regla general refiere expresamente: "El responsable tendrá la obligación de informar a los titulares de los datos, la información que recaba de ellos y con qué fines, a través del aviso de privacidad".

Por su parte la fracción II define a las bases de datos para efectos de esta ley con relación a su contenido (datos personales) y la finalidad con la que serán tratados los datos en ellas contenidos. Lo anterior conforme a lo establecido por el artículo 3 del Reglamento, es decir, soportes físicos o electrónicos que hagan posible su acceso con arreglo a criterios determinados, independientemente de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Enseguida, la fracción III hace referencia al bloqueo, el cual consiste en la identificación y guarda de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de cumplir con la obligación legal de conservación y con el fin de impedir cualquier otro tratamiento distinto, por el plazo de prescripción legal o el plazo establecido contractualmente, para que transcurridos se proceda a su supresión, entendida de acuerdo con los términos establecidos en el Reglamento de la Ley como "actividad consistente en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas por el responsable".

El maestro Santiago Barajas Montes de Oca indica que la prescripción legal se refiere a un modo de adquirir el dominio de cosa ajena a través de su posesión durante cierto tiempo y con los requisitos marcados por la ley, o de liberarse de una obligación que se hubiese contraído y cuyo cumplimiento no se exija durante el término que señale la Ley.[31] Por su parte el artículo 1135 del Código Civil Federal establece que "es un medio de adquirir bienes o de liberarse de obligaciones, mediante el transcurso de cierto tiempo y bajo las condiciones establecidas por la ley".

Con relación al plazo contractual, consideramos oportuno remitirnos al concepto de "contrato" que nos proporciona el maestro Francisco M. Cornejo

[31] Barajas, S. (2005). Prescripción de acciones, en el *Diccionario Jurídico Mexicano P-Z del Instituto de Investigaciones Jurídicas*. México. Porrúa-UNAM, pp. 2969-2970.

Certucha quien indica que proviene del latín *contractus,* derivado a su vez del verbo *contrahere,* reunir, lograr, concertar.[32] Se trata de un acto jurídico bilateral que se constituye por el acuerdo de voluntades de dos o más personas y que produce ciertas consecuencias jurídicas (creación o transmisión de derechos y obligaciones) debido al reconocimiento de una norma de derecho. Sin embargo, tiene una doble naturaleza, pues también presenta el carácter de norma jurídica individualizada.

Según la maestra Alicia Elena Pérez Duarte, el término "plazo" deriva del latín *plactium,* convenido término o tiempo señalado para una cosa. Se trata de una de las modalidades a que puede estar sujeta una obligación, es el plazo o término definido como un acontecimiento futuro de realización cierta al que está sujeta la eficacia o extinción de una obligación.[33]

A mayor abundamiento, nos expone que el legislador emplea ambos conceptos como sinónimos, sin embargo, la doctrina los distingue que: el término es el momento en que ha de cumplirse o extinguirse una obligación y el plazo es el lapso en el cual puede realizarse, en otras palabras, el término es el fin del plazo.

Por último, consideramos oportuno establecer que el bloqueo se refiere a un periodo de tiempo durante el cual los datos personales no podrán ser objeto de tratamiento, y que una vez transcurrido, lo procedente es llevar a cabo la supresión en la base de datos respectiva.

La fracción IV se refiere al "consentimiento". En términos generales, el maestro Lisandro Cruz Ponce nos expone que el consentimiento es el acuerdo de dos o más voluntades destinadas a producir consecuencias o fines de interés legal en la celebración de cualquier convenio o contrato.[34]

De conformidad con el artículo 1792 del Código Civil Federal, "convenio" es el acuerdo de dos o más voluntades para crear, transferir, modificar o extinguir obligaciones. A su vez, el artículo 1793 agrega que cuando las convenciones producen o transfieren obligaciones y derechos toman el nombre de "contratos".

El consentimiento es un requisito de existencia del contrato, conforme a lo señalado en los artículos 1794 y 2224 del Código Civil Federal, si no existe consentimiento, no habrá contrato.

---

[32] Cornejo, F. (2005). Contrato, en el *Diccionario Jurídico Mexicano A-C del Instituto de Investigaciones Jurídicas*. México. Porrúa-UNAM, p. 831.

[33] Pérez, A. (2005). Plazo, en el *Diccionario Jurídico Mexicano P-Z del Instituto de Investigaciones Jurídicas*. México. Porrúa-UNAM, p. 2882.

[34] Cruz L. (2005). Consentimiento, en el *Diccionario Jurídico Mexicano A-C del Instituto de Investigaciones Jurídicas*. México. Porrúa-UNAM, p. 779.

De especial interés resulta el hecho de que, conforme al criterio del autor citado, el consentimiento nace en el instante en que legalmente se produce el acuerdo de voluntades de las partes que intervienen en una relación jurídica en formación, o sea, cuando coinciden entre sí las voluntades individuales, de cada uno de los interesados.[35]

Por otro lado, el artículo 1803 del Código Civil Federal reconoce que el consentimiento es expreso cuando la voluntad se manifiesta por escrito y por medios electrónicos. De esta forma, la voluntad que se expresa mediante la firma electrónica, así como la autógrafa digitalizada constituye un medio válido para expresar el consentimiento expreso y dar validez a los actos realizados por el firmante y debe entenderse, en este último caso, que se trata del consentimiento expresado por escrito capturado en un medio electrónico.

En el mismo sentido, el artículo 1834 bis del mismo ordenamiento reconoce que los contratos que requieran forma escrita y firma otorgada por las partes cumplirán dichos requisitos cuando se utilicen medios electrónicos siempre que la información generada en forma (i) íntegra, (ii) sea atribuible a las personas obligadas y (iii) accesible para su ulterior consulta.

Por lo que se refiere a la calidad probatoria de la firma electrónica, el artículo 79 del Código Federal de Procedimientos Civiles establece que para conocer la verdad el juzgador puede valerse de cualquier cosa o documento sin más limitaciones que las pruebas estén reconocidas por la Ley y tengan relación inmediata con los hechos controvertidos.

El artículo 210-A del Código Federal de Procedimientos Civiles reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. También establece que para valorar la fuerza probatoria de la información se estimará la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible, atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Dicho artículo también establece que cuando la Ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

[35] Ídem.

Por último, y no por ello menos importante, el Reglamento de la Ley en su artículo 12 establece las características que debe tener el consentimiento para ser considerado válido en materia de protección de datos, es decir, debe ser libre, específico e informado, además el consentimiento expreso debe ser también inequívoco. Al respecto cabe hacer la siguiente reflexión, ¿puede una norma reglamentaria ir más allá de las previsiones de una ley general?

Las fracciones V y VI se encuentran estrechamente relacionadas, la primera de ellas se refiere al género: datos personales y la segunda a la especie: datos personales sensibles. Previamente hemos revisado la definición de "datos personales", en consecuencia, procedemos al análisis de los datos personales sensibles, sobre el particular debemos subrayar que se dividen en dos categorías generales: a) los que afecten a la esfera más íntima de su titular y b) los que su utilización indebida puede dar origen a discriminación o conlleve un riesgo grave.

Particularmente, el legislador considera sensibles aquellos datos que pueden revelar aspectos como: el origen racial o étnico, el estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual. En consecuencia, los responsables deberán estar muy atentos a la necesidad de requerir dicha información, así como el uso y el trato que se le dará una vez recabada.

Este punto es muy importante ya que, de pretender ser originariamente un concepto objetivo (el origen racial o étnico, el estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual) la propia definición legal lo convierte en subjetivo (los que afecten a la esfera más íntima de su titular y los que su utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste), por lo tanto, no sólo es necesario hablar de datos sensibles, sino de igual manera debemos hacer referencia al tratamiento sensible y cuidadoso de la información.

La fracción VII indica que cuando en el conjunto normativo se haga referencia a días, se tratará de días hábiles, sin hacer mayor aclaración al respecto. Lo cual nos remite al contenido del artículo 5 del conjunto normativo objeto de estudio, donde se precisa que, a falta de disposición expresa en esta Ley, se aplicarán de manera supletoria las disposiciones del Código Federal de Procedimientos Civiles y de la Ley Federal de Procedimiento Administrativo.

Al respecto, tenemos que remitirnos al artículo 281 del Código Federal de Procedimientos Civiles donde se precisa que las actuaciones judiciales se practicarán en días y horas hábiles y que son días hábiles todos los del año, menos los domingos y aquéllos que la ley declare festivos.

De forma más exhaustiva, el artículo 28 de la Ley Federal de Procedimiento Administrativo dispone que en los plazos fijados en días no se contarán los inhábiles, salvo disposición en contrario. No se considerarán días hábiles: los sábados, los domingos, el 1 de enero, 5 de febrero, 21 de marzo, 1 y 5 de mayo, 1 y 16 de septiembre, 20 de noviembre, 1 de diciembre de cada seis años, cuando corresponda a la transmisión del Poder Ejecutivo Federal y 25 de diciembre, así como los días en que tengan vacaciones generales las autoridades competentes o aquellos en que se suspendan las labores, lo que se hará del conocimiento público mediante acuerdo del titular de la dependencia respectiva y que se publicará en el *Diario Oficial de la Federación* (DOF).

La fracción VIII se refiere al término "disociación" y lo refiere como un procedimiento para lograr que la información que se obtenga, o que en su momento se trate, no pueda asociarse a persona identificada o identificable. En relación con este concepto, el maestro Ignacio Medina Lima lo define como el sustantivo plural (procedimientos) cuya raíz latina es *procedo, processi,* proceder, adelantarse, avanzar. En general, nos dice que "procedimiento" es la manera de hacer una cosa o de realizar un acto.[36]

Dicho concepto corresponde a *procédure* en francés, *procedure* en inglés, *procedura* en italiano y *verfahren* en alemán, de donde podemos desprender la generalidad del uso de la figura jurídica de referencia en los múltiples sistemas jurídicos.[37]

No obstante, consideramos que el ordenamiento legal objeto de análisis se refiere a la concepción general que se desprende del *Diccionario de la Lengua Española*, al entender el procedimiento como la acción de proceder o al método de ejecutar algo, en la especie, la forma en que los datos personales dejan de asociarse a su titular. La disociación sólo implica la falta de vinculación con el titular del derecho, aún y cuando el dato no pierda su origen. El procedimiento de disociación permitirá el anonimato del dato y por consecuencia el despojo de identidad del origen del mismo. Este procedimiento se vuelve medular para la publicidad del dato sin que medie consentimiento. Una vez que los datos son disociados del titular, el responsable puede utilizarlos sin restricciones para finalidades estadísticas y, desde luego, para efectos de difusión de la información. Los responsables deberán incorporar procedimientos de disociación de datos y permearlos al seno de su organización estableciendo los mecanismos adecuados, suficientes y pertinentes para que, en el caso de la publicación de datos estadísticos o bien en proyectos de *big data,* estos no puedan volver a asociarse con el titular causándole un perjuicio.

[36] Medina, I. (2005). Procedimientos, en el *Diccionario Jurídico Mexicano P-Z del Instituto de Investigaciones Jurídicas*. México. Porrúa-UNAM, p. 3056.
[37] Ídem.

Las fracciones IX, XIV, XVI y XVII se refieren a los diversos sujetos que intervienen en el tratamiento de datos personales a saber: *Encargado*, *Responsable*, *Tercero* y *Titular.* Estas definiciones, como se verá en el resto del trabajo, cobran especial relevancia pues definen los diversos roles que en la materia cobran acción. Cada uno de ellos tiene relevancia en la relación jurídica que surge a partir del tratamiento de datos personales. Es indiscutible que los protagonistas en esta relación serán el titular y el responsable, en donde en principio la relación de tratamiento se perfecciona. Desde luego sin restar importancia a las otras figuras que son definidas por la ley.

La fracción X nos indica en qué consiste una fuente de acceso público, misma que corresponde a las bases de datos cuya consulta puede ser realizada por cualquier persona, sin mayor requisito que, en su caso, el pago de una contraprestación de conformidad con lo señalado por el Reglamento de la Ley que en su artículo 7 dispone que se consideran fuentes de acceso público:

a) Los medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general.
b) Los directorios telefónicos en términos de la normativa específica.
c) Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa.
d) Los medios de comunicación social.

Para que los supuestos enumerados en dicho artículo sean considerados fuentes de acceso público será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contraprestación, derecho o tarifa. No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita. El tratamiento de datos personales obtenidos a través de fuentes de acceso público respetará la expectativa razonable de privacidad a la que se refiere el tercer párrafo del artículo 7 de la Ley.

Respecto a la fracción XI del artículo que se analiza encontramos que cuando se haga referencia a Instituto se trata del Instituto Federal de Acceso a la Información y Protección de Datos a que hace referencia la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Actualmente, se refiere al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) que es el organismo constitucional autónomo garante del cumplimiento de dos derechos fundamentales: el de acceso a la información pública y el de protección de datos personales.

Para el primero, garantiza que cualquier autoridad en el ámbito federal, órganos autónomos, partidos políticos, fideicomisos, fondos públicos, sindicatos o cualquier persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad entregue la información pública que le soliciten.

Para el segundo, garantiza el uso adecuado de los datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición que toda persona tiene con respecto a su información.

Por lo que respecta a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, encontramos que fue publicada en el *Diario Oficial de la Federación* el 11 de junio de 2002. Sin embargo, fue abrogada por la Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el *Diario Oficial de la Federación* el 9 de mayo de 2016. La última reforma se publicó el 27 de enero de 2017, misma que en su artículo 1 indica:

> La presente Ley es de orden público y tiene por objeto proveer lo necesario en el ámbito federal, para garantizar el derecho de acceso a la Información Pública en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos federales o realice actos de autoridad, en los términos previstos por la Constitución Política de los Estados Unidos Mexicanos y la Ley General de Transparencia y Acceso a la Información Pública.

El artículo 2 del ordenamiento legal en cita señala como objetivos de dicho ordenamiento los siguientes:

I. proveer lo necesario para que todo solicitante pueda tener acceso a la información mediante procedimientos sencillos y expeditos;

II. transparentar la gestión pública mediante la difusión de la información oportuna, verificable, inteligible, relevante e integral;

III. favorecer la rendición de cuentas a los ciudadanos, de manera que puedan valorar el desempeño de los sujetos obligados;

IV. regular los medios de impugnación que le compete resolver al Instituto;

V. fortalecer el escrutinio ciudadano sobre las actividades sustantivas de los sujetos obligados;

VI. consolidar la apertura de las instituciones del Estado mexicano, mediante iniciativas de gobierno abierto que mejoren la gestión pública a través de la difusión de la información en formatos abiertos y accesibles, así como la participación efectiva de la sociedad en la atención de los mismos;

VII. propiciar la participación ciudadana en la toma de decisiones públicas, a fin de contribuir a la consolidación de la democracia, y

VIII. promover y fomentar una cultura de transparencia y acceso a la información pública.

Las fracciones XII y XIII aclaran que las referencias a Ley y reglamento en el ordenamiento legal que se estudia se refieren a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y al Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares respectivamente, mientras que la fracción XV indica que al mencionar Secretaría, se refiere a la Secretaría de Economía, misma que de conformidad con el artículo 41 del mismo ordenamiento legal, tendrá como función difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano, promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital y el desarrollo económico nacional en su conjunto.

La Secretaría de Economía en su carácter de autoridad reguladora, función que pueden ejercer otras dependencias también en el ámbito de sus respectivas competencias, coadyuvada por el Instituto, tiene las siguientes funciones:

- Emisión de la regulación que corresponda
- Regulación de las bases de datos de comercio automatizadas o que formen parte de un proceso de automatización
- Emisión de los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad
- Desarrollo de los mecanismos y medidas de autorregulación
- Registros de consumidores en materia de datos personales y verificar su funcionamiento

Luego de haber relacionado los conceptos medulares que servirán para interpretar la Ley, las disposiciones generales incluyen un repertorio de limitaciones contenidas en las mismas. Del texto de este artículo, que casi copia textualmente lo dispuesto en el segundo párrafo del artículo 16 constitucional, se desprende que existe una obligación, por mandato constitucional, consistente en que la ley que regule el derecho a la protección de datos personales deberá

establecer 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.

Sin embargo, para que dichas excepciones puedan utilizarse se tendrán que desarrollar en instrumentos de rango legislativo para cumplir con lo que señala la norma constitucional, es decir, señalar específicamente cuáles son esos supuestos de excepción referidos de manera general y justificarlos para guardar armonía en todo el marco jurídico. Su omisión limita el ejercicio de derechos humanos y, por tanto, puede dejar sin efectos el esquema de excepciones a los principios al no desarrollar los respectivos supuestos ordenados por la Constitución.

En su última parte, las disposiciones generales de este cuerpo normativo y derivado de la naturaleza jurídica que adquirió el INAI con la reforma constitucional del 7 de febrero de 2014, dicho organismo quedó fuera de la administración pública federal y en razón de ello es que se tomó la postura de que las resoluciones que emite en los procedimientos que se sustancian ante él, a saber el de protección de derechos y los procedimientos de verificación e imposición de sanciones no pueden ser revisadas por el Tribunal Federal de Justicia Administrativa, sino vía amparo directo, pues considera que el referido tribunal no tiene competencia para analizar resoluciones emitidas por un organismo con autonomía constitucional.[38]

La problemática que se presenta en este punto es que, no obstante que se le otorgó autonomía constitucional al Instituto, el legislador no derogó los artículos 56 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares así como el 126 y 138 de su reglamento, los cuales establecen que el medio de impugnación en contra de las resoluciones emitidas por el Instituto es el juicio de nulidad ante el Tribunal Federal de Justicia Administrativa y siendo que la actuación de todas las autoridades debe ajustarse al principio de legalidad a efecto de garantizar la seguridad jurídica de los gobernados, es que el Instituto queda obligado a aplicar los artículos referidos y, como consecuencia de ello, a establecer en sus resoluciones que el medio de

[38] En ese sentido se recomienda revisar los criterios jurisprudenciales dictados por la Suprema Corte de Justicia de la Nación provenientes de las controversias constitucionales 32/2005 y 31/200, las cuales llevan como título *Órganos constitucionales autónomos. Sus características y Órganos constitucionales autónomos. Notas distintivas y características,* respectivamente. Publicado en el *Semanario Judicial de la Federación* y su gaceta. Tomo XXVII. Febrero de 2008. Tesis: P./J. 12/2008. Página: 1871 y Tomo XXV. Mayo de 2007. Tesis: P./J. 20/2007, p. 1647. Por su parte existe una tesis aislada de un tribunal colegiado de circuito que refiere la competencia del Tribunal Federal de Justicia Administrativa titulada *Resoluciones definitivas en materia de responsabilidades administrativas de los servidores públicos dictadas por los órganos constitucionales autónomos.* El Tribunal Federal de Justicia Administrativa es competente para conocer del juicio de nulidad promovido en su contra (legislación vigente a partir del 19 de julio de 2016). Dicha tesis se puede encontrar en *Gaceta del Semanario Judicial de la Federación.* Libro 51. Febrero de 2018. Tomo III. Tesis: I.1o.A.196 A (10a), p. 1540.

impugnación que procede en contra de sus determinaciones es el juicio de nulidad.

No obstante, el Instituto, dentro de los juicios de nulidad que actualmente se están sustanciando en el Tribunal Federal de Justicia Administrativa, está haciendo valer como causal de improcedencia la "supuesta" falta de competencia del referido tribunal para revisar resoluciones emitidas por organismos con autonomía constitucional, misma que no ha prosperado a la fecha, ya que no se ha generado jurisprudencia alguna que determine que el Tribunal es incompetente para tales efectos. Tampoco se han derogado los preceptos legales que establecen dicha vía de impugnación, y aunado a ello, se destaca que el Instituto ha interpuesto diversos recursos de revisión fiscal en contra de las sentencias emitidas por el referido Tribunal Federal de Justicia Administrativa, mismos que han sido desechados por diversos tribunales colegiados del Poder Judicial de la Federación por considerarlos improcedentes.

No cabe duda que dicho tema genera polémica y posiciones encontradas, pues si bien es cierto que es discutible el argumento de la supuesta falta de competencia que hace valer el Instituto, no es menos cierto que derivado de la aplicación estricta del principio de legalidad (elevado a rango de derecho humano) y de garantizar la seguridad jurídica de los gobernados, no resulta dable considerar que se pudieran desechar los juicios de nulidad que se interpongan contra sus resoluciones, pues de ser así, no se aplicarán disposiciones jurídicas vinculantes en detrimento de los particulares, lesionando su esfera jurídica y haciendo nugatorio el ejercicio de su derecho humano de acceso efectivo a la justicia, además de que, tal y como se estableció con antelación, el Poder Judicial de la Federación no ha realizado ningún pronunciamiento que ratifique la postura jurídica del Instituto.

Conclusiones

El primer antecedente que podemos encontrar en una ley federal respecto a la protección de los datos personales data del año 2002 y lo podemos encontrar en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Sin embargo, este derecho fundamental se reconoce como tal a partir de 2009 con reformas a los artículos 16 y 73 constitucionales en los que se otorga reconocimiento a la protección de datos personales como garantía individual y se faculta al Congreso de la Unión para legislar en la materia. Constituyendo un derecho humano fundamental subjetivo, autónomo y de tercera generación.

Del análisis del artículo 2 se concluye que los sujetos obligados llamados "responsables" son quienes llevan a cabo el tratamiento de datos personales

con excepción de las sociedades de información crediticia y aquellos que sean recabados con fines exclusivamente personales y sin fines de divulgación o uso comercial. De igual manera, las disposiciones generales que son objeto de este comentario se encargan de elaborar un listado de definiciones que constituyen los conceptos fundamentales y básicos a los que se deberá atender al momento de interpretar y aplicar la Ley en los supuestos que marca la misma.

Un apartado importante de este capítulo es el establecimiento de las limitaciones al derecho de autodeterminación informativa ya que, como sabemos, ningún derecho es absoluto, por tanto, el legislador en el artículo 4 de la ley en comento, establece los límites y las excepciones en la aplicación del derecho a la protección de los datos personales: seguridad nacional, orden, seguridad y salud públicas y derechos de los terceros, lo cual es consistente con el tipo de derecho que pretendemos proteger. Al igual que sucede con la máxima publicidad como principio, la máxima privacidad encuentra los límites típicos de la información. Cuando hablamos del derecho a la vida privada debemos tener en consideración, como sucede con otros derechos, que no hablamos de derechos absolutos o cerrados a los cuales no pueden ponerse límites, por el contrario y partiendo desde una idea no absoluta, encontraremos que la Ley refiere al menos cuatro límites, los cuales se encuentran orientados, no sólo a aspectos vinculados con el interés público, como podrían ser la seguridad nacional, el orden o la salud pública, sino también a objetivos legítimos vinculados a particulares como sucede con los derechos de terceros. Ello se traduce en acciones concretas que la misma ley recogerá en su articulado respecto a la difusión de la información sin consentimiento del titular en donde se pretenden proteger justamente los asuntos de interés público o bien los derechos de terceros.

Por último, cabe destacar que la supletoriedad contenida en estas disposiciones generales surge con la finalidad de integrar las omisiones que existan en una determinada ley o con la finalidad de interpretar disposiciones en forma que se integre con sus principios generales para subsanar las lagunas, por lo que tratándose del Instituto Nacional de Acceso a la Información es un caso particular ya que se trata de un órgano constitucional autónomo.

Referencias

Barajas, S. (2005). Prescripción de acciones, en *Diccionario Jurídico Mexicano P-Z.* Instituto de Investigaciones Jurídicas. México. Porrúa-UNAM. Pp. 2969-2970.

Cornejo, F. (2005). Contrato, en *Diccionario Jurídico Mexicano A-C.* Instituto de Investigaciones Jurídicas. México. Porrúa-UNAM, p. 831.

Cruz, L. (2005). Consentimiento, en *Diccionario Jurídico Mexicano A-C*. Instituto de Investigaciones Jurídicas. México. Porrúa-UNAM, México, p. 779.

García, F. (2005). Derecho privado y derecho público, en *Diccionario Jurídico Mexicano.* Instituto de Investigaciones Jurídicas. México. Porrúa-UNAM, p. 1229.

Medina, I. (2005). Procedimientos, en *Diccionario Jurídico Mexicano P-Z.* Instituto de Investigaciones Jurídicas. México. Porrúa-UNAM, p. 3056.

Pérez, A. (2005). Plazo, en *Diccionario Jurídico Mexicano* P-Z Instituto de Investigaciones Jurídicas. México. Porrúa-UNAM, p. 2882.

Sitios web

RAE. (2017). *Procedimiento, en Diccionario de la Lengua Española.* Recuperado de: *http://dle.rae.es/?id=UErw6id*. Fecha de consulta: 15 de octubre 2018.

INAI. (s.f). ¿Qué es el INAI? Recuperado de: *http://inicio.ifai.org.mx/SitePages/que-es-el-inai.aspx*. Fecha de consulta: 15 de octubre 2018.

____. (s.f). ¿Qué es el INAI? Recuperado de: *http://inicio.ifai.org.mx/SitePages/que-es-el-inai.aspx.* Fecha de consulta: 15 de octubre 2018.

Fuentes legales

Constitución Política de los Estados Unidos Mexicanos. *Diario Oficial de la Federación*, 5 de febrero de 1917. Última reforma publicada el 27 de agosto de 2018.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. *Diario Oficial de la Federación*, 11 de junio de 2002. Última reforma publicada el 18 de diciembre de 2015. Ley abrogada el 9 de mayo de 2016.

Ley Federal de Transparencia y Acceso a la Información Pública. *Diario Oficial de la Federación*, 9 de mayo de 2016. Última reforma publicada el 27 de enero de 2017.

Ley Federal de Procedimiento Administrativo. *Diario Oficial de la Federación*, 4 de agosto de 1994. Última reforma publicada el 2 de mayo 2017.

Ley para Regular las Sociedades de Información Crediticia. *Diario Oficial de la Federación*, 15 de enero de 2002. Última reforma publicada el día 8 de marzo 2018.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*, 21 de diciembre 2011.

Código Federal de Procedimientos Civiles. *Diario Oficial de la Federación*, 24 de febrero de 1943. Última reforma publicada el 9 de abril 2012.

Código Civil Federal. *Diario Oficial de la Federación* (publicado en cuatro partes), 26 de mayo, 14 de julio, 3 y 31 de agosto de 1928. Última reforma publicada el 9 de marzo 2018.

CAPÍTULO II
DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO II
DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

Artículo 6. *Los responsables en el tratamiento de datos personales deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.*

Artículo 7. *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 Ley.

Artículo 8. *Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.*

El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente Ley.

El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.

Artículo 9. *Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.*

No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

Artículo 10. *No será 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;
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, o
VII. Se dicte resolución de autoridad competente.

Artículo 11. *El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.*

Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.

El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

Artículo 12. *El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.*

Artículo 13. *El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.*

Artículo 14. *El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, 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. El responsable deberá tomar las medidas 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.*

Artículo 15. *El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.*

Artículo 16. *El aviso de privacidad deberá contener, al menos, la siguiente información:*

I. La identidad y domicilio del responsable que los recaba;
II. Las finalidades del tratamiento de datos;
III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;

V. En su caso, las transferencias de datos que se efectúen, y
VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta ley.

En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

Artículo 17. *El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:*

I. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y
II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo anterior, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

Artículo 18. *Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el cambio en el aviso de privacidad.*

No resulta aplicable lo establecido en el párrafo anterior, cuando el tratamiento sea con fines históricos, estadísticos o científicos.

Cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados, en consideración al número de titulares, o a la antigüedad de los datos, previa autorización del Instituto, el responsable podrá instrumentar medidas compensatorias en términos del reglamento de esta ley.

Artículo 19. *Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.*

Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta

el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Artículo 20. *Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas 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.*

Artículo 21. *El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.*

COMENTARIO

Cynthia Solís Arredondo

Introducción

El presente trabajo busca proponer una fundamentación de los principios que irradian del derecho a la autodeterminación informativa previsto en nuestra Constitución y que han dado origen legal al tratamiento de datos personales, tanto en lo público como en lo privado.

Se ha pretendido hablar, en un primer momento, de los principios en materia de protección de datos como origen y motor de este nuevo derecho para contextualizar al lector sobre todo el andamiaje previo que ha supuesto la construcción del derecho que nos ocupa. Se ha partido de la base de que el derecho a la vida privada no puede ser soslayado por todo aquel que aborda los temas de protección de datos personales.

A partir de ello se ha tratado de proponer una revisión de cada uno de los principios que refieren los ordenamientos jurídicos en materia de protección de datos, esperando que al lector le pueda servir como una referencia importante para el desarrollo de los múltiples aspectos que de ellos se derivan.

Correlaciones

Principio de licitud. Artículo 10 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP).
Principio de consentimiento. Artículos 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 del RLFPDPPP.

Principio de información. Artículos 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35 del RLFPDPPP.
Principio de calidad. Artículos 36, 37, 38, 39 del RLFPDPPP.
Principio de finalidad. Artículos 40, 41, 42, 43 del RLFPDPPP.
Principio de lealtad. Artículo 44 del RLFPDPPP.
Principio de proporcionalidad. Artículos 45 y 46 del RLFPDPPP.
Principio de responsabilidad. Artículos 47, 48, 49, 50, 51, 52, 53, 54, 55 del RLFPDPPP.

Análisis de contenido

Los principios de una ley son la columna vertebral sobre la que se sostienen las disposiciones de ésta, aquella inspiración del legislador, basada en los más altos valores universales del bien común, el orden público y el Estado de derecho,[39] una ley que carece de principios, no puede ser jurídica ni moralmente válida.

En este orden de ideas, los principios de una ley son, en gran medida, los que soportan la validez de todos los derechos y obligaciones de los interesados, por esto es importante ahondar en ellos para entender los pilares de la legislación que habremos de conocer y, sobre todo, aplicar. No es sino hasta que comprendemos el valor que existe detrás de algo, cuando nos es más sencillo acatar las obligaciones que conlleva.

Hablando de textos de derecho internacional, el artículo 12 de la Declaración de los Derechos Humanos de 1948 dispone que: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

En el caso de la hoy derogada Directiva Europea 95/46/CE, en su artículo 6 estableció, en su momento, los principios relativos a la calidad de los datos y en el artículo 7, los principios relativos a la legitimación del tratamiento de datos, y que, en su momento sirvieron de inspiración de la ley mexicana, puesto que se interpretan y se recogen en ésta y es el motivo de plasmarlos en la presente obra literaria.

La Directiva Europea antes mencionada enumeraba los siguientes principios:

[39] Sistema de información legislativa. (s.f.) *Estado de derecho*. Recuperado de: *http://sil.gobernacion.gob.mx/Glosario/definicionpop.php?ID=97*. Fecha de consulta: 31 de octubre 2018.

I. Principios relativos a la calidad de los datos:

A) Los datos deben ser tratados de manera leal y lícita. Al respecto, queda claro que la lealtad a la que se refiere esta disposición, es al apego a la ley con la que debe llevarse a cabo el tratamiento, en complemento de la licitud de éste.

B) Serán recogidos con fines determinados, explícitos y legítimos. Uno de los principios universalmente reconocidos es el de la autodeterminación informativa, para ello es fundamental que el responsable de los datos establezca y declare, de manera precisa y explícita, los fines para los cuales llevará cabo el tratamiento de datos, de una manera legítima. Queda claro que, en algunos casos excepcionales, hay datos cuya finalidad puede desviarse ligeramente, pero en ningún caso deberá ser incompatible con los fines originalmente estipulados.

C) Deberán ser exactos y cuando sea necesario actualizarlos. Este principio vigila que aquellos datos inexactos o incompletos puedan ser debidamente rectificados o en su caso suprimidos.

D) Deberán conservarse de forma tal que la identificación de los individuos interesados no exceda el tiempo razonable para cumplir con los fines para los que originalmente fueron recogidos.

II. Principios relativos a la legitimación del tratamiento de datos:

E) Todo tratamiento de datos deberá llevarse a cabo sólo si el interesado ha manifestado su consentimiento de forma inequívoca.

F) El tratamiento podrá llevarse a cabo si es necesario para la ejecución de un contrato, aplicación de medidas precontractuales o a petición del interesado.

G) Podrá efectuarse en caso de que sea necesario para proteger el interés vital del interesado.

H) Si el tratamiento de datos es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público.

I) Cuando el tratamiento que se lleve a cabo sea necesario para la satisfacción de un interés legítimo del responsable o del tercero siempre que no afecten el derecho a la intimidad de los titulares.

Por su parte, la Convención Europea para la Protección de los Derechos del Hombre y las Libertades Fundamentales de 1950, en su artículo 8 dice: “La vida privada y familiar incluye la intimidad del domicilio y la inviolabilidad de la correspondencia. Regula en qué casos puede haber una injerencia de los poderes públicos en estos derechos”.

El tema también se recoge en la Carta de los Derechos Fundamentales de la Unión Europea que figura en el artículo 5 del Tratado sobre la Unión Europea desde el 2009.

En su artículo 7 declara la obligación del respeto a la vida privada y familiar: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".

En su artículo 8 menciona expresamente la protección de datos de carácter personal:

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.

Por su parte, el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter personal y su protocolo adicional relativo a las autoridades de control y a los flujos transfronterizos de datos, mejor conocido como Convenio 108,[40] al que México se adhirió en el mes de junio de 2018,[41] establece de forma puntual los límites al tratamiento automatizado de datos y a su flujo transfronterizo, de forma tal que los países firmantes se comprometen a contar con una legislación local equivalente o congruente con el convenio, a efecto de garantizar la seguridad de los datos personales sin frenar, en la medida de lo posible, la economía.

Los principios básicos de esta normativa se encuentran en el capítulo II y, aunque casi todos se reducen a la calidad de los datos, haciendo un comparativo con la legislación mexicana, los principios que logramos identificar en este texto son los siguientes:

- Lealtad y licitud: los datos deberán ser obtenidos de manera leal y legítima.
- Finalidad: los datos deberán ser tratados para finalidades determinadas y no podrán ser utilizados de forma incompatible con dichas finalidades.

[40] Recuperado de: *http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf* Fecha de consulta: 2 de octubre 2018.

[41] Recuperado de: *http://dof.gob.mx/nota_detalle.php?codigo=5526265&fecha=12/06/2018*. Fecha de consulta: 2 de octubre 2018.

- Proporcionalidad: los datos que se recaben deberán ser adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se han obtenido los datos, además deberán ser conservados de tal forma que se permita identificar al titular de los datos durante el tiempo de conservación que no podrá ser mayor que aquel necesario para las finalidades para las cuales se han obtenido.
- Calidad: los datos que se traten deberán ser exactos y actualizados.
- Deber de seguridad: se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Como es de advertir, en los textos precedentes existe una diferencia remarcable entre el derecho a la vida privada y el derecho a la protección de los datos personales que retomaremos constantemente durante este trabajo. No todos los datos de carácter personal son privados, sobre todo aquellos elementos de identidad como nombre, imagen, características físicas, etc.

Desde que nacemos, nuestros padres nos incorporan, de una u otra manera, a la vida pública, ya sea porque se nos asigna un nombre, una filiación, una nacionalidad y, en general, datos que nos identificarán el resto de nuestra vida, que desde que nuestros padres o tutores nos dan de alta en un registro público, estos serán accesibles para todos los interesados durante el resto de nuestra vida, o gracias a la tecnología, mucha información nace y permanecerá en internet o en redes sociales, la cual dará la vuelta al mundo infinidad de veces y vivirá ahí de forma totalmente indefinida y técnicamente incontrolable.[42]

Por lo tanto, reiteramos que existe una gran cantidad de información que, de hecho, o de derecho, no contempla la esfera de nuestra vida privada. Privacidad no es lo mismo que protección de datos, aunque vayan, comúnmente, de la mano.

Entrando en materia de la ley mexicana, el capítulo II de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y del capítulo II del Reglamento abordan y detallan estos principios rectores.

[42] Independientemente de los derechos que nos amparan respecto de la protección de nuestros datos personales, no hay que olvidar que las plataformas tecnológicas conocidas como “redes sociales” basan su éxito en la transmisión y réplica masiva de información. Por lo tanto, una vez que esa información entra a internet, técnicamente hablando, sale de nuestro control, puesto que no es posible impedir que alguien la descargue, copie o reproduzca de cualquier manera, sin tener rastro de ello.

Cada uno de los principios contemplados en ella revisten una importancia y trascendencia particular, sin embargo, se encuentran interconectados y en muchas ocasiones son interdependientes, por lo que se recomienda tener siempre en cuenta que la exigencia en el cumplimiento de cada uno de los principios de manera aislada es igual de importante que en su conjunto. Esto se hace patente al momento en que la autoridad garante, en el procedimiento de imposición de sanciones, califica el incumplimiento, tanto de la Ley como de los principios, y por esto, muchas de las sanciones se incrementan significativamente. En ese tenor refiere la ley mexicana:

> Artículo 6.- Los responsables en el tratamiento de datos personales deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

En nuestra legislación son ocho principios los que se recogen de la inspiración de la normativa europea, tanto de la directiva como de legislación local, principalmente de la española, y se prevé que en México se reconocerán ocho grandes principios que regirán el tratamiento de datos personales por parte de los particulares. Cabe destacar que en otros países en vez de ocho son cuatro, o a veces seis, en realidad lo que pretendió el legislador fue desdoblar algunos principios y convertirlos en dos o tres, a efecto de perseguir la precisión en su aplicación. Veamos cada uno de ellos:

Principio de licitud

La licitud debe comprenderse en su sentido más amplio, es decir, que tal y como lo establece el artículo 10 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante RLFPDPPP o Reglamento); no sólo debemos limitarnos al cumplimiento cabal de esta Ley, sino a toda la legislación nacional e internacional aplicable en el caso particular.

Por ejemplo, las instituciones financieras deben atender a lo dispuesto por la Ley, su reglamento, la Ley de Instituciones de Crédito, las disposiciones de carácter general aplicables a las instituciones de crédito (Circular Única de Bancos), Ley de Sociedades de Información Crediticia, la normativa de la Secretaría de Hacienda y del Banco de México, etc. y garantizar el cumplimiento armonizado de cada una de las disposiciones legales que le sean aplicables.

La obtención de los datos no debe hacerse a través de medios engañosos o fraudulentos, es decir, el responsable deberá, no sólo establecer mecanismos trasparentes de obtención de datos, sino que la redacción del aviso de privacidad debe ser clara y precisa, evitando palabras que puedan inducir al error al titular.

Asimismo, este artículo nos habla de un concepto un tanto subjetivo: la expectativa razonable de privacidad. Este concepto tiene mucho que ver con la confianza y confidencialidad natural que debe mediar entre el responsable y el titular, ya que este último, como la parte más vulnerable de la relación, le encomienda el tratamiento de sus datos personales al responsable, única y exclusivamente para los fines primarios de la relación jurídica que los vincula.

Es por ello que, aunque parezca banal su cumplimiento, es fundamental conocer la totalidad de normativas que el responsable debe cumplir durante todo el ciclo de vida del tratamiento de los datos personales.

Principio de consentimiento

El consentimiento de forma genérica se entiende como la manifestación de la voluntad. El *Diccionario de Real Academia Española*, en su tercera acepción, hace una interesante referencia específica al consentimiento en el ámbito del derecho: "Manifestación de voluntad, expresa o tácita, por la cual un sujeto se vincula jurídicamente".[43] En este caso titular y responsable son las partes implicadas en la relación jurídica.

El consentimiento es la puerta de entrada al tratamiento lícito de datos personales, salvo en los casos de excepción, el responsable está obligado a poner a disposición del titular el aviso de privacidad correspondiente, para luego así, poder solicitar y obtener su consentimiento.

El artículo 11 del Reglamento puntualiza que el consentimiento debe ir referido a una finalidad determinada dentro del aviso de privacidad, por lo que el responsable debe ser claro y explícito al momento de describir los fines que dará a los datos.

En relación con el artículo 12 del Reglamento, el consentimiento debe contar con las siguientes características:

- Ser libre, es decir, sin que medien vicios de la voluntad
- Específico, que refiera a finalidades puntuales
- Informado, que consiste en hacer saber del aviso de privacidad al titular

Además de esto, debe ser inequívoco, lo que implica que el responsable deberá probar de manera indubitable el consentimiento.

[43] RAE. (2018). Consentimiento, en *Diccionario de la Lengua Española.* Recuperado de: *http://dle.rae.es/?id=AP6QLrg*. Fecha de consulta: 13 de septiembre de 2018.

La Ley prevé dos tipos de consentimiento: el tácito y el expreso. Se entiende que el consentimiento es expreso cuando existe una exteriorización y señales manifiestas de éste, ya sea verbalmente, por escrito, por medios electrónicos o por signos que no dejen lugar a duda el consentimiento. Por ejemplo, en el caso de avisos de privacidad puestos a disposición vía telefónica, un sí equivalente a oprimir alguna tecla del teléfono. Por otro lado, si no existe requerimiento de solicitar el consentimiento expreso en la Ley por el tipo de datos o de finalidades, basta con obtener o presumir el consentimiento tácito.[44]

Gracias a los nuevos modelos de negocio y las tecnologías de la información y la comunicación es posible que el responsable no recabe de manera directa los datos, sino que lo haga a través de terceros o de medios electrónicos, en cuyo caso, el plazo para que el titular se oponga a las finalidades secundarias del tratamiento, es de cinco días en términos del artículo 14 del Reglamento, luego de este plazo se entenderá que hay consentimiento tácito salvo prueba en contra. Por ejemplo, que el titular demuestre que nunca se puso a su disposición el aviso de privacidad. La carga de la prueba del consentimiento recae en todo momento en el responsable.

Respecto a los datos sensibles, el responsable debe obtener y acreditar el consentimiento para el tratamiento de este tipo de datos, ya sea a través de su firma autógrafa, electrónica o autenticándose de alguna manera (por ejemplo, *token* electrónico de un sólo uso).

No podrán generarse bases de datos sensibles, a menos que existan fines legítimos, concretos y acordes que así lo justifiquen en relación con las actividades del sujeto regulado. El segundo párrafo de la Ley está relacionado con los principios de finalidad y de proporcionalidad.

El principio de consentimiento sí admite supuestos de excepción, toda vez que la naturaleza de algunos servicios y medios de contacto conducen a dicha excepcionalidad. De igual manera en otras circunstancias existen imposibilidades técnicas o fácticas, además de que en muchas ocasiones los titulares buscando la protección de sus derechos pueden pretender oponerse al tratamiento de datos personales que son fundamentales para la relación jurídica, o al interés público, o por ministerio de Ley.

Principio de calidad

Las bases de datos que se generen deben tener mantenimiento, es decir, que constantemente deben revisarse y actualizarse, esto con la finalidad de que la información contenida en ellas sea pertinente, correcta y actualizada.

[44] "Que no se entiende, percibe, oye o dice formalmente, sino que se supone e infiere". Recuperado de: *http://dle.rae.es/srv/search?m=30&w=tácito*. Fecha de consulta: 7 de septiembre 2018.

Asimismo, muchas de las finalidades para las que se recaban datos personales suelen ser temporales, por ejemplo, con relación a las referencias laborales, sólo se justifica conservar la información durante el período de contratación, puesto que se entiende que es el momento en el que el candidato está sujeto a evaluación, posteriormente, y una vez que se convierte en empleado, los datos de contacto de las referencias laborales ya no tienen razón de existir en el expediente laboral. De la misma manera, respecto de la información relativa a incumplimiento contractual, ésta debe eliminarse en un plazo de 72 meses.

En relación con los artículos 36, 37, 38 y 39 del Reglamento, el responsable debe establecer plazos razonables para la conservación de la información de carácter personal, y una vez agotados los plazos debe proceder a su supresión.

Principio de finalidad

Para cumplir cabalmente con el principio de consentimiento, las finalidades plasmadas en el aviso de privacidad deben ser lícitas, precisas y congruentes con la naturaleza de la relación jurídica entre el responsable y el titular, luego entonces, cuando el responsable pretenda tratar los datos personales del titular para fines distintos a los expresados inicialmente, se deberá solicitar y obtener de nuevo su consentimiento.

El artículo 41 establece la diferencia entre finalidades primarias y secundarias, ya que las primeras son indispensables para dar origen y mantener la relación jurídica, mientras que las segundas no lo son, y si el titular se opone al tratamiento de sus datos para éstas últimas, el responsable está obligado a acatar su voluntad, sin que por ello se concluya la relación jurídica o se niegue el establecimiento de ella.

Principio de proporcionalidad

Por regla general la normativa en esta materia se basa en un criterio de minimización del tratamiento de datos personales, es decir, que se limite a lo mínimo indispensable y obedece a la simple lógica de que a mayor número de datos y de procesos de tratamiento, mayor es el nivel de riesgo de la información. Este criterio de minimización lo encontramos expresamente en el artículo 46 del Reglamento. Es así que el responsable debe llevar a cabo tareas y esfuerzos razonables para limitar el número de datos y el tiempo de tratamiento de éstos.

Principio de lealtad

Desde que se obtiene el dato hasta que se suprime, el responsable está comprometido con su correcto tratamiento, ya sea personalmente o a través de

terceros, cumpliendo y haciendo cumplir los principios de la Ley y asegurándose de que el citado tratamiento se lleve a cabo, en todo momento, conforme al aviso de privacidad original.

Principio de información

La base primordial de la autodeterminación informativa es justamente la información clara y precisa respecto del tratamiento de datos personales. La principal obligación del responsable (aunque no por ello la más importante) es la de informar a los titulares acerca de todos y cada uno de los datos personales que se recaban y para qué. El medio idóneo de información es precisamente el aviso de privacidad y es por ello que esta obligación no admite excepción.

Además de los elementos mínimos para los avisos de privacidad enlistados en el artículo 16 de la Ley, el Reglamento precisa que, ante todo, el aviso de privacidad debe ser sencillo, con la información necesaria y expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento, para ello, el responsable deberá crear un aviso de privacidad congruente con el nivel de compresión del titular, al que va dirigido, absteniéndose de utilizar lenguaje sofisticado y frases ambiguas. De la misma manera, el artículo 26 del Reglamento, complementa los elementos mínimos que debe contener el aviso de privacidad, que son los artículos 8, 15, 16, 33 y 36 de la Ley, así como los que se establezcan en los lineamientos a que se refiere el artículo 43, fracción III.[45]

Por regla general, el aviso de privacidad debe ser puesto a disposición del titular previo al tratamiento de sus datos, sin embargo, no siempre se recaban los datos de manera directa y presencial, existe una gran cantidad de plataformas electrónicas mediante las cuales se recaban datos personales, así que la Ley, en el segundo párrafo de este artículo, establece los lineamientos mínimos para la comunicación del aviso de privacidad en estos casos y se complementa con los artículos 27, 28 y 29 del Reglamento.

La entrada en vigor de la Ley, el 6 de julio de 2010, planteaba muchas interrogantes acerca de su implementación. Una de ellas fue su aplicación respecto a la información recabada y tratada con anterioridad. En realidad, la única complejidad objetiva que se planteaba era la de establecer contacto y comunicación con titulares cuyos datos estaban en posesión de los responsables, décadas antes de que siquiera se planteara esta ley, para ello, el legislador y el ejecutivo federal establecieron la posibilidad de implementar

[45] DOF. (2013, enero 17). *Lineamientos del Aviso de Privacidad*. Recuperado de: *http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013* Fecha de consulta: 20 de septiembre de 2018.

medidas compensatorias. Los mecanismos para su diseño, solicitud e implementación se detallan en los artículos 32, 33, 34 y 35 del Reglamento.

Cabe señalar que, a la fecha de la publicación de la presente obra, es poco probable la autorización de medidas compensatorias, toda vez que para acreditar la imposibilidad de hacer del conocimiento del aviso de privacidad a los titulares, se requeriría de circunstancias excepcionales y argumentos suficientes.

Principio de responsabilidad

La palabra responsabilidad tiene su origen en el latín *responsum* que significa responder; implica la habilidad de responder, de tal suerte que el responsable, tal y como se acota en esta obra, entre otras tantas obligaciones, debe rendir cuenta del correcto tratamiento de los datos personales que tiene en su poder, para ello debe implementar medidas administrativas, técnicas y físicas que protejan los datos personales evitando en la medida de lo posible y razonable, la pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. El detalle de todas las tareas preliminares que debe llevar a cabo el responsable, a efecto de cumplir con este principio, se encuentra en el artículo 48 del Reglamento.

No obstante, existen diferentes documentos de referencia generados por el INAI, que aunque no son obligatorios, son obras de consulta sumamente importantes para la aplicación de este principio. A continuación, enlistaremos un par de ellos:

1. *Recomendaciones en materia de seguridad de datos personales*.[46]
2. *Manual en materia de seguridad de datos personales para Mipymes y organizaciones pequeñas*.[47]

Hoy en día ningún sujeto responsable está exento de sufrir una vulneración de seguridad a las bases de datos personales. Sin embargo, deberá llevar a cabo una valoración del impacto de dicha vulneración al titular respecto de sus datos personales, por lo que, si el responsable estima que afecta de manera significativa a los derechos patrimoniales o morales del titular, deberá informárselo de manera inmediata para encontrarse en aptitud de tomar las medidas que considere pertinentes a efecto de defender sus derechos.

---

[46] IFAI. (s.f.). *Recomendaciones en materia de seguridad de datos personales*. Recuperado de: *http://www.dof.gob.mx/nota_detalle_popup.php?codigo=5320179* Fecha de consulta: 10 de septiembre 2018.

[47] IFAI. (2014). *Manual en materia de seguridad de datos personales para Mipymes y organizaciones pequeñas*. Recuperado de: *http://inicio.ifai.org.mx/nuevo/Manual%20seguridad%20MIPYMES.pdf* Fecha de consulta: 10 de septiembre 2018.

Principio de confidencialidad

El término confidencialidad, proviene de la palabra confianza, la cual depositan los titulares en el responsable para que éste trate sus datos personales de manera diligente, con base en la expectativa mínima de privacidad que debe guardarse dentro de la relación titular–responsable.

Esta confianza se extiende a que el tratamiento de datos que declaró el responsable a través de su aviso de privacidad es, con exactitud, lo que efectivamente llevará a cabo, incluyendo las finalidades para las cuales se realice la transferencia de datos a terceros, y más aún, esta obligación de guardar la confianza del titular se extiende y aplica a los terceros receptores de la información, incluso después de haber finalizado una relación contractual.

La confidencialidad es un elemento clave y una pieza fundamental de la seguridad de la información. Ese compromiso de secrecía debe primar en toda relación contractual y es por ello que, durante todo el ciclo de vida del dato personal, el responsable debe de llevar a cabo todas las acciones y medidas necesarias para que no se vea afectada la cualidad de confidencialidad de los datos personales.

Referencias

Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Recuperado de: *http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf* Fecha de consulta: 2 de octubre 2018.

Solis, C. (2018). *Usurpación de identidad digital: un estudio comparativo de soluciones francesas, mexicanas y norteamericanas*. Université Paris-Saclay.

Laffaire, M. (2005). *Protection de données à caractère personnel*. Francia. Éditions d'Organisation.

Mattatia, F. (2013). *Traitement des données personnelles. Le guide juridique*. Francia. Eyrolles.

Tenorio, G. et al. (2012). *Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares*. México. Porrúa-Universidad Panamericana.

Sitios web

Diccionario de la RAE. (2018). Concepto de "consentimiento". Recuperado de: *http://dle.rae.es/?id=AP6QLrg* Fecha de consulta: 13 de septiembre 2018.

_____. (2018). Concepto de "tácito". Recuperado de: *http://dle.rae.es/srv/search?m=30&w=tácito* Fecha de consulta: 7 de septiembre 2018.

DOF. (2013, enero 17). *Lineamientos del Aviso de Privacidad*. Recuperado de: *http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013* Fecha de consulta: 20 de septiembre 2018.

IFAI. (2014). *Manual en materia de seguridad de datos personales para Mipymes y organizaciones pequeñas*. Recuperado de: *http://inicio.ifai.org.mx/nuevo/Manual%20seguridad%20MIPYMES.pdf* Fecha de consulta: 10 de septiembre 2018.

_____. (s.f.). *Recomendaciones en materia de seguridad de datos personales*. Recuperado de: *http://www.dof.gob.mx/nota_detalle_popup.php?codigo=5320179* Fecha de consulta: 10 de septiembre 2018.

Sistema de Información Legislativa. (s.f.) *Estado de derecho*. Recuperado de: *http://sil.gobernacion.gob.mx/Glosario/definicionpop.php?ID=97* Fecha de consulta: 31 de octubre 2018.

_____. (s.f.) *Estado de derecho*. Recuperado de: *http://sil.gobernacion.gob.mx/Glosario/definicionpop.php?ID=97* Fecha de consulta: 31 de octubre 2018.

CAPÍTULO III
DE LOS DERECHOS DE LOS TITULARES DE DATOS PERSONALES

CAPÍTULO III
DE LOS DERECHOS DE LOS TITULARES DE DATOS PERSONALES

Artículo 22. *Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.*

Artículo 23. *Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento.*

Artículo 24. *El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos.*

Artículo 25. *El titular tendrá en todo momento el derecho a cancelar sus datos personales.*

La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.

Una vez cancelado el dato se dará aviso a su titular.

Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el

responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también.

Artículo 26. *El responsable no estará obligado a cancelar los datos personales cuando:*

I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;
II. Deban ser tratados por disposición legal;
III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;
IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;
V. Sean necesarios para realizar una acción en función del interés público;
VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y
VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

Artículo 27. *El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular.*

COMENTARIO

Héctor Guzmán Rodríguez

Introducción

El reconocimiento de los derechos de los titulares frente a los responsables del tratamiento de datos personales constituye uno de los pilares sobre los cuales descansan los sistemas de protección de datos más conocidos, avanzados y longevos del mundo. No se trata de derechos universalmente reconocidos y, por esta razón, debemos estudiar su naturaleza, contenido y alcance desde varios puntos de vista, incluida su regulación en algunos ámbitos internacionales.

Un análisis de derecho comparado permite comprobar que existen iniciativas internacionales que, desde hace décadas, han impulsado el

reconocimiento y regulación de los derechos de los titulares frente a empresas u otras entidades que han obtenido y tratan sus datos personales. Asimismo, podemos encontrar que cada país cuenta con una normativa sobre protección de datos que regula los derechos de los titulares, concediendo a éstos más o menos facultades frente a los responsables.

Conforme a lo anterior, dentro de la presente introducción proponemos tener en cuenta las siguientes disposiciones normativas internacionales que desde su emisión han regulado algún tipo de derecho relativo al control que los titulares pueden tener sobre sus datos personales:

- Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (datan de 1980 y fueron actualizadas en 2013) que desde su versión original establecieron el "Principio de Participación Individual", conforme a la cual, y de manera general, reconocía el derecho de las personas para obtener confirmación de un responsable de datos personales (*data controller*) sobre si éste trata o no sus datos personales. El mismo principio reconocía el derecho del titular para solicitar la eliminación, corrección o compleción de sus datos ante el responsable.
- Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), (1981) que en su artículo 8 establece una serie de "garantías complementarias para el titular de datos personales", incluyendo la posibilidad de conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal del responsable de dicho fichero; el derecho a confirmar la existencia del fichero automatizado de datos y la comunicación de dichos datos de forma inteligible; obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción al derecho interno que haga efectivos los principios de protección que prevé el propio Convenio.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo (24 de octubre de 1995), relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que en su artículo 12 (Derecho de acceso) reguló el derecho de los interesados para obtener del responsable del tratamiento "la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos",

así como, en su caso, "la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones" de dicha directiva.

- El marco de privacidad de la APEC (Asia-Pacific Economic Cooperation), (2005), que desde su versión original reconoció como principio (VIII) el acceso y corrección de la información personal de las personas, para que puedan obtener confirmación sobre su tratamiento por parte de un responsable específico, la información personal en posesión del responsable y, en su caso, la rectificación, compleción, enmienda o eliminación de su información personal.

Las referencias anteriores permiten observar que los derechos de los titulares han existido y evolucionado en diversas partes del mundo, donde en el mes de septiembre de 2018 sabemos que en nuestro país se mantiene la misma regulación que fue establecida desde la publicación de la LFPDPPP en julio de 2010, la cual analizaremos en el presente capítulo.

Cabe señalar que, si bien es cierto que este trabajo se centra en el contenido de la LFPDPP, no debemos olvidar que desde el 1 de junio de 2009 los derechos de acceso, rectificación, cancelación y oposición sobre el tratamiento de los datos personales están reconocidos de manera expresa en nuestra Constitución Política, estableciendo, en el mismo momento de su reconocimiento, que su ejercicio será regulado en los términos que fije la ley.[48]

Precisamente en México los derechos de los titulares forman parte del contenido de un derecho de mayor envergadura y alcance: el derecho a la autodeterminación informativa, donde el ejercicio y cumplimiento de cada uno de los derechos ARCO[49] otorga sentido a dicha autodeterminación, en la medida en que los titulares de datos personales pueden conocer las finalidades y el tipo de datos en posesión de un responsable, rectificar o actualizar sus datos, solicitar su cancelación y, en su caso, oponerse a su tratamiento.

Así pues, analizaremos las características esenciales de estos derechos y de las limitaciones que existen para su ejercicio, se harán recomendaciones organizativas que permitan a los responsables el ejercicio de estos derechos en la forma y dentro de los plazos legalmente establecidos, referencias de derecho comparado y, en su caso, recomendaciones adoptadas por la autoridad encargada de la aplicación de la LFPDPPP.

[48] Cfr. Artículo 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos.

[49] Aunque en el presente capítulo podamos referirnos a ellos como los derechos ARCO, no olvidemos que la definición legal de este acrónimo de uso común en España fue aportada por el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (artículo 2, fracción II).

Correlaciones

Artículo 22:
Artículos 2, fracción III, 87, 88, 90, 91, 92, 93, 94, 95, 96, 97, 98 y 100 del Reglamento de la LFPDPPP.
Lineamientos, vigésimo, fracción VIII y vigésimo octavo de los lineamientos del aviso de privacidad.
Artículo 23:
Artículos 99, 101 y 102 del Reglamento de la LFPDPPP.
Lineamientos, vigésimo, fracción VIII y vigésimo octavo de los lineamientos del aviso de privacidad.
Artículo 24:
Artículos 103 y 104 del Reglamento de la LFPDPPP.
Lineamientos, vigésimo, fracción VIII y vigésimo octavo de los lineamientos del aviso de privacidad.
Artículo 25:
Artículos 105, 106 107 y 108 del Reglamento de la LFPDPPP.
Lineamientos, vigésimo, fracción VIII y vigésimo octavo de los lineamientos del aviso de privacidad.
Artículo 26:
Artículos 105, 106 107 y 108 del Reglamento de la LFPDPPP.
Artículo 27:
Artículos 109, 110 y 111 del Reglamento de la LFPDPPP.
Lineamientos, vigésimo, fracción VIII y vigésimo octavo de los lineamientos del aviso de privacidad.

Análisis de contenido

Los derechos ARCO. Características, medios de ejercicio y medidas organizativas

Elevados a concepto jurídico, definidos en el artículo 2, fracción II del Reglamento de la LFPDPPP, los derechos ARCO constituyen el conjunto de potestades reconocidas a favor de los titulares para que puedan solicitar y ejercer control sobre sus datos personales en posesión de cualquier responsable sujeto a sus disposiciones.

Acuñado en España, la sigla ARCO engloba los derechos que, de manera conjunta o independiente, pueden ser ejercidos por un titular para obtener información sobre la persona que tiene posesión de sus datos personales, el tipo de datos objeto de tratamiento, las finalidades dicho tratamiento, el destino de éstos en caso de haber sido transferidos, así como para actualizarlos, corregirlos, solicitar su eliminación y, en determinados casos, oponerse a su tratamiento.

Las disposiciones del artículo 22 de la LFPDPPP, 87 y 89 de su reglamento establecen dos características esenciales de los derechos ARCO: son personales y son independientes entre sí.

El ejercicio de los derechos ARCO podrá realizarse por cualquier titular (o por su representante legal), pero sólo en relación con sus datos personales. Nadie puede solicitar el acceso, rectificación, cancelación u oponerse al tratamiento de los datos personales de otra persona. En tales casos, los responsables tienen el derecho y deber de negar una solicitud de este tipo.[50]

En el caso de menores de edad, personas incapacitadas o en estado de interdicción serán las personas que los representen, quienes deberán ejercer, en su nombre, los derechos ARCO conforme a las reglas de representación establecidas en el Código Civil Federal.

La autonomía de los derechos ARCO —que reconoce el mismo artículo 22— forma parte de su naturaleza y características. Desde que estos derechos fueron esbozados en los ochenta, su regulación se ha construido de forma que el ejercicio de uno no condicione el ejercicio de los demás, en otras palabras y por ejemplo: no es necesario que para el ejercicio del derecho de oposición debamos ejercer en primer lugar nuestro derecho de acceso, ni el ejercicio previo de nuestro derecho de rectificación puede impedir que, de manera simultánea o posterior, podamos ejercer el derecho de acceso a nuestros datos personales.

Las reglas para acreditar la identidad de las personas que ejercen cualquiera de los derechos ARCO[51] prevén el uso de medios comunes y corrientes para realizarlo (original y copia para cotejo de un documento de identificación), instrumentos electrónicos u otros mecanismos de autenticación permitidos por otras disposiciones normativas e incluso medios establecidos por el propio responsable. De manera expresa se prevé el uso de firmas electrónicas avanzadas que eximen de la presentación de cualquier copia de nuestro documento de identificación.

El régimen de representación para el ejercicio de estos derechos es bastante simple: copia del documento de identificación del representado y representante, instrumento público o carta poder e, incluso, declaración en comparecencia personal del titular.

Aunque desde una perspectiva muy tecnológica, algunos medios de acreditación de la identidad pudieran parecer arcaicos, no debemos olvidar dos factores esenciales contenidos a lo largo de las disposiciones del régimen de protección de datos de nuestro país: (i) resulta aplicable para bases de

[50] Ver artículo 34, fracción I de la LFPDPPP.
[51] Ver artículo 89 del Reglamento de la LFPDPPP.

datos no automatizadas y (ii) toma en cuenta a cualquier colectivo de titulares, incluidos aquellos que no tienen relación con los responsables de sus datos a través de medios electrónicos de ningún tipo.

Sobre los documentos de identificación que los titulares pueden aportar al momento de ejercer alguno de sus derechos, los responsables pueden tener en cuenta que el INAI ha indicado lo siguiente:

> El responsable, en todo momento, se encontrará obligado a cerciorarse de la identidad del titular que pretenda ejercer sus derechos de acceso, rectificación, cancelación y oposición, así como también para los casos en los que el titular busque revocar su consentimiento; para lo anterior, será indispensable que el titular presente cualquiera de las siguientes identificaciones:
>
> - Credencial del Instituto Nacional Electoral.
> - Pasaporte.
> - Cartilla del servicio militar nacional.
> - Cédula profesional.
> - Cartilla de identidad postal (expedida por Sepomex).
> - Certificado o constancia de estudios.
> - Constancia de residencia.
> - Credencial de afiliación del IMSS.
> - Credencial de afiliación al ISSSTE.
> - Documento migratorio que constate la legal estancia del extranjero en el país.[52]

Si bien es cierto que los derechos ARCO son derechos personales que se extinguen con sus dueños, existen grandes dudas sobre su ejercicio en representación de personas fallecidas, cuando por diversos motivos existe algún tipo interés para solicitar el acceso, rectificación, cancelación o solicitar la oposición al tratamiento de los datos de un difunto.

Al respecto, recordemos que ni la LFPDPPP ni su reglamento se refieren, de forma expresa, a la protección de los datos personales de personas fallecidas, aunque también es cierto que el artículo 53, fracción I del primer ordenamiento establece que una solicitud de protección de derechos será sobreseída cuando el titular de datos fallezca. Sin embargo, en su *Guía para titulares de los datos personales*, el INAI se ha referido al tema en los siguientes términos:

En cuanto a los datos personales de una persona fallecida, sólo la persona que acredite tener interés jurídico, conforme a las leyes aplicables, podrá ejercer los derechos ARCO, siempre que el titular de los datos personales

[52] IFAI. (2011). *Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO*, p. 7.

hubiere expresado fehacientemente su voluntad o exista un mandato judicial al respecto, y se trate de una solicitud presentada ante un responsable del sector público.[53]

La normativa establece una obligación a cargo de los responsables para que sean ellos mismos los que determinen los medios para el ejercicio de los derechos ARCO (artículo 90 del Reglamento de la LFPDPPP), en los que la simplicidad y la facilitación del ejercicio para los titulares deben ser ejes de su configuración.

Por lo tanto, se deberán poner a disposición de los titulares "medios remotos o locales de comunicación electrónica u otros que (el responsable) considere pertinentes", pudiendo establecer "formularios, sistemas y otros medios simplificados para facilitar a los titulares el ejercicio de los derechos ARCO". De todo ello deberán informar los responsables en sus respectivos avisos de privacidad.[54]

De manera contemporánea a la realidad que se pretende regular, el artículo 91 del Reglamento de la LFPDPPP se refiere de forma expresa a los servicios de atención al público para indicar que los responsables que cuenten con este tipo de servicios podrán atender solicitudes para el ejercicio de los derechos ARCO a través de los mismos. Desde luego que el reto para cualquier responsable que decida utilizar estos servicios de atención para recibir solicitudes de derechos ARCO será la capacitación del personal para atenderlas en tiempo y forma, conforme a un proceso documentado, implementado y debidamente revisado.

En este sentido, resulta de suma importancia el último párrafo del artículo 22 de la LFPDPPP, ya que sus disposiciones tienen un contenido eminentemente organizacional, orientado a garantizar el respeto de los derechos de los titulares. Este párrafo constata que el cumplimiento de las disposiciones de la Ley no se limita a la emisión de avisos de privacidad y alguna que otra cláusula contractual, sino que para su cumplimiento los responsables deben asumir o adoptar medidas que permitan el ejercicio sin dilación de los derechos ARCO, es decir, adoptar medidas técnicas y administrativas para el resguardado de los datos personales, que permitan su ejercicio sin dilación.

¿Cómo se deben resguardar los datos personales para evitar la dilación a que se refiere el artículo 22 de referencia? La respuesta no puede ser unívoca, ya que depende de diversos factores que incluyen el tamaño y actividad del

[53] INAI. (2017). *Guía para titulares de los datos personales*. Vol. 3, p.11. Recuperado de: *http://corpusiurispdp.inai.org.mx/iberoamericano/OtrosDocumentos/Guia%20Titulares-03_PDF.pdf#search=ARCO*

[54] Cfr. Artículo 90 del Reglamento de la LFPDPPP y 28 de los Lineamientos del Aviso de Privacidad.

responsable, así como las finalidades y el tipo de datos que son tratados por éste. No obstante, sí es posible proponer acciones de cumplimiento para que los responsables desplieguen acciones organizativas que les permitan contar con procesos y personas o unidades de atención capacitadas para dar atención a estas solicitudes:[55]

- Establecer medios de atención que garanticen la recepción de todas las solicitudes, evitando la centralización de funciones en una sola persona y/o medio de recepción.
- Contar con políticas y procedimientos para su atención.
- Establecer programas de capacitación para la debida atención de los derechos ARCO.
- Supervisar el cumplimiento de esas políticas.
- Revisarlas periódicamente.
- Disponer de mecanismos de cumplimiento y sanción en caso de incumplimiento de las políticas de atención de derechos ARCO.
- Establecer medidas de trazabilidad de los datos personales para saber, en todo tiempo, quién y para qué finalidades está tratando los datos personales.
- Contar con un inventario de bases de datos.

Finalmente, debemos tener presente que los derechos ARCO podrán restringirse por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros, tal y como está expresamente previsto por el segundo párrafo del artículo 16 constitucional y por el artículo 88 del reglamento de la LFPDPPP. Este último indica que esta restricción tendrá lugar "en los casos y con los alcances previstos en las leyes aplicables en la materia, o bien mediante resolución de la autoridad competente debidamente fundada y motivada".

Por consiguiente, y tal y como veremos a continuación, el estudio de los derechos ARCO no sólo requiere conocer de su existencia y de los medios para su ejercicio, sino que debe abarcar el estudio de sus restricciones particulares para cada uno de ellos, las cuales podrán ser invocadas por los responsables para negar de manera fundada y motivada una solicitud a la que se ha dado trámite.

Poner a disposición los medios y recursos que sean necesarios para atender solicitudes de derechos ARCO puede resultar una tarea ardua y costosa en función al grado de organización y madurez del responsable que desea implementar un procedimiento efectivo de atención. Sin embargo, el

[55] Es decir, cumplir con el principio de responsabilidad para el tratamiento de datos personales, en aquellos aspectos relativos a la atención y cumplimiento de solicitudes de ejercicio de derechos ARCO.

costo de dicha implementación no puede ni debe ser trasladado a los titulares, ya que el ejercicio de los derechos ARCO será gratuito, con excepción de la cobertura de gastos relacionados con el envío, reproducción y, en su caso, certificación de documentos, y a menos que en el caso del derecho de acceso el titular ejerza dicho derecho más de una vez durante un período menor a doce meses, en este caso se cobrará un costo cuyo monto no debe exceder del equivalente a tres unidades de medida y actualización.[56]

En cuanto a las generalidades de los derechos ARCO, concluyamos indicando que los responsables deben dar trámite a toda solicitud sobre el ejercicio de cualquier derecho ARCO, con independencia de que tenga o no tenga los datos del titular ejerciente bajo su posesión; en estos últimos casos el responsable deberá contestar dentro del plazo legal y en el marco de las disposiciones a que se refiere el siguiente capítulo de esta obra.

Derecho de acceso

En su concepto más elemental, el derecho de acceso (artículo 23 de la LFPD-PPP) constituye la facultad de un titular de datos personales para solicitar, de cualquier responsable, determinada información sobre el tratamiento de sus datos personales, incluso en aquellos casos en que el titular no está seguro de la identidad exacta del responsable y/o del número o tipo de datos que son objeto de tratamiento.

La redacción del artículo 23 (antes indicado) es sumamente amplia y se refiere, tanto al derecho de los titulares para "acceder a sus datos personales que obren en poder del responsable", como a la facultad para "conocer el Aviso de Privacidad al que está sujeto el tratamiento" (de sus datos personales); esto último, en aparente contradicción al principio de información.

No existe contradicción si un titular ejerce el derecho de acceso para conocer qué datos personales son tratados por un responsable y al mismo tiempo exige conocer el aviso de privacidad que regula su tratamiento. En determinados casos es posible que un titular pueda presumir que sus datos no fueron obtenidos de manera lícita y desea saber, a través de dicho aviso, cuáles son las finalidades del tratamiento y el resto de información que ese documento debe contener.[57]

Por su parte, y de manera nuevamente amplia, el artículo 101 del Reglamento de la LFPDPPP establece que este derecho también faculta al titular para obtener "información relativa a las condiciones y generalidades del tratamiento", donde a la fecha no existe ningún criterio judicial que aclare

[56] Cfr. artículos 35 de la LFPDPPP y 93 del Reglamento de la LFPDPPP.
[57] Cfr. artículo 16 de la LFPDPPP.

cuál es el contenido o alcance de los conceptos, condiciones y generalidades del tratamiento.

No obstante lo anterior, el INAI sí ha desarrollado recomendaciones y directrices al respecto y en dos documentos distintos indica lo siguiente:

> El poder de disposición o decisión que tiene el titular sobre la información que le concierne, conlleva necesariamente el derecho de acceder y conocer si su información personal está siendo objeto de tratamiento, así como el alcance, condiciones y generalidades de dicho tratamiento. De esta manera, el responsable debe garantizar al titular su derecho de acceso en tres vías:
>
> - La primera implica que el titular pueda conocer la efectiva existencia del tratamiento a que son sometidos sus datos personales.
> - La segunda, que el titular pueda tener acceso a sus datos personales que están en posesión del responsable.
> - La tercera, supone el derecho a conocer las circunstancias esenciales del tratamiento, lo cual se traduce en el deber que tiene el responsable de informar al titular sobre el tipo de datos personales tratados; todas y cada una de las finalidades que justifican el tratamiento; las personas que intervienen en el tratamiento (encargados); en caso de transferencias, los destinatarios, las finalidades de las mismas, la información personal transferida, entre otra información que el titular esté interesado en conocer.[58]

> Es el derecho que tienes de solicitar, que el acceso a tus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como de conocer información relacionada con el uso que se da a tu información personal.
> Por ejemplo, podrías solicitar a tu banco, acceso a tus datos de contacto que tenga registrados, para comprobar que los mismos sean correctos y estén actualizados. También, podrías solicitar a la organización o institución para la que trabajes, acceso a tu expediente laboral o a cualquier documento específico contenido en éste.[59]

Nuestra normativa dispone que el derecho de acceso se dará por cumplido cuando el responsable ponga a disposición del titular solicitante los datos personales en sitio, o bien mediante la expedición de copias simples, medios magnéticos, ópticos, sonoros, visuales, holográficos o utilizando otras tecnologías de la información que se hayan previsto en el aviso de privacidad.

---

58 IFAI. (2011). *Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO*, p. 8.

59 INAI. (2017). *Guía para Titulares de los Datos Personales*. Volumen 3, p. 6.

Conforme a lo anterior, corresponde a cada responsable determinar, en el marco de sus propias actividades y recursos, de qué manera podrá cumplir con esta obligación en caso de recibir este tipo de solicitudes.

Un ejercicio de derecho comparado, con aspectos prácticos sobre los alcances del derecho de acceso, nos permite comprobar que la Agencia Española de Protección de Datos proporciona la siguiente información sobre el alcance del derecho de acceso:

> El derecho de acceso es tu derecho a dirigirte al responsable del tratamiento para conocer si está tratando o no tus datos de carácter personal y, en el caso de que se esté realizando dicho tratamiento, obtener la siguiente información:
> - Una copia de tus datos personales que son objeto del tratamiento.
> - Los fines del tratamiento.
> - Las categorías de datos personales que se traten.
> - Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular, los destinatarios en países terceros u organizaciones internacionales.
> - El plazo previsto de conservación de los datos personales, o si no es posible, los criterios utilizados para determinar este plazo.
> - La existencia del derecho del interesado a solicitar al responsable: la rectificación o supresión de sus datos personales, la limitación del tratamiento de sus datos personales u oponerse a ese tratamiento.
> - El derecho a presentar una reclamación ante una Autoridad de Control.
> - Cuando los datos personales no se hayan obtenido directamente de ti, cualquier información disponible sobre su origen.
> - La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y al menos en tales casos, información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de ese tratamiento para el interesado.
> - Cuando se transfieran datos personales a un tercer país o a una organización internacional, tienes derecho a ser informado de las garantías adecuadas en las que se realizan las transferencias.[60]

Además, en su *Guía para el Ciudadano*, la misma Agencia Española aclara que el acceso remoto, directo y seguro a los datos personales constituye una forma de atención a la solicitud de acceso a datos personales:

> Se entenderá otorgado este derecho si el responsable te facilita un sistema de acceso remoto, directo y seguro a tus datos personales que garantice el acceso

[60] Agencia Española de Protección de Datos. Portal Oficial. Sección Ejerce Tus Derechos. Recuperado de: *https://www.aepd.es/reglamento/derechos/index.html.*

a su totalidad. La comunicación por el responsable del modo en que puedas acceder a dicho sistema se considerará por atendida tu solicitud.[61]

En complemento de este ejercicio de derecho comparado, resulta interesante comprobar que el Reglamento General de Protección de Datos de la Unión Europea desglosa, de manera exhaustiva, el tipo de información que un titular (interesado) puede obtener al ejercer su derecho de acceso:

Artículo 15

Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;
b) las categorías de datos personales de que se trate;
c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
f) el derecho a presentar una reclamación ante una autoridad de control;
g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
h) 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.[62]

Por otro lado, podemos encontrar que la Unión Europea no considera que el derecho de acceso comprende el derecho a requerir y obtener copia de documentos específicos o de todos los documentos de una persona contenidos en una base de datos específica.

[61] Agencia Española de Protección de Datos. (2018). *Guía para el Ciudadano*, p. 20. Recuperado de: *https://www.aepd.es/media/guias/guia-ciudadano.pdf*

[62] Reglamento General de Protección de Datos. Recuperado de: *https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32016R0679*

En los asuntos acumulados C-141/12 y C-372/12, la tercera sala del Tribunal de Justicia de la Unión Europea (TJUE) resolvió sobre los siguientes aspectos:

- Protección de las personas físicas en lo que respecta al tratamiento de datos personales.
- Directiva 95/46/CE, artículos 2, 12 y 13.
- Concepto de "datos personales".
- Extensión del derecho de acceso del interesado.
- Datos relativos al solicitante de un documento de residencia y análisis jurídico incluidos en un documento administrativo preparatorio de la resolución.
- Carta de los Derechos Fundamentales de la Unión Europea, artículos 8 y 41.

En los considerandos correspondientes, el TJUE expuso los siguientes razonamientos:

> (55) El artículo 8 de la Carta, que garantiza el derecho a la protección de los datos personales, establece en su apartado 2, en particular, que toda persona tiene derecho a acceder a los datos recogidos que le conciernan. Aplica este requisito el artículo 12, letra a), de la Directiva 95/46 (véase, en este sentido, la sentencia Google Spain y Google, EU:C:2014:317, apartado 69).
> (56) Esta disposición de la Directiva 95/46 establece que los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento, libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos, la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos.
> (57) Aunque la Directiva 95/46 obliga, de este modo, a los Estados miembros a garantizar que los interesados puedan obtener del responsable del tratamiento de datos personales la comunicación de todos los datos de este tipo que trate que les conciernan, deja a dichos Estados la tarea de determinar la forma material concreta que debe adoptar esa comunicación, siempre que sea «inteligible», es decir, que permita a los interesados conocer esos datos y comprobar que son exactos y son tratados de conformidad con esa Directiva, para que dichas personas puedan ejercer, en su caso, los derechos que los artículos 12, letras b) y c), 14, 22 y 23 de la misma les confieren (véase, en este sentido, la sentencia Rijkeboer, EU:C:2009:293, apartados 51 y 52).
> (58) Por tanto, en la medida en que puede cumplirse plenamente el objetivo perseguido por ese derecho de acceso mediante otra forma de comunicación, el interesado no puede obtener ni del artículo 12, letra a), de la Directiva 95/46 ni del artículo 8, apartado 2, de la Carta el derecho a recibir una copia del documento o del fichero original en el que figuran esos datos. Para no dar acceso al interesado a información distinta de los datos personales que le conciernan,

> éste puede recibir una copia del documento o del fichero original en el que se haya imposibilitado la lectura de esa otra información.
> (59) En situaciones como las que dan lugar a los litigios principales, de la respuesta dada en el apartado 48 de la presente sentencia se desprende que sólo son «datos personales» en el sentido del artículo 2, letra a), de la Directiva 95/46 los datos relativos al solicitante del documento de residencia que figuran en la minuta y, en su caso, los que figuran en el análisis jurídico incluido en dicha minuta. En consecuencia, el derecho de acceso que puede invocar ese solicitante en virtud del artículo 12, letra a), de la Directiva 95/46 y del artículo 8, apartado 2, de la Carta se refiere únicamente a esos datos. Para dar cumplimiento a este derecho de acceso, basta con facilitar al solicitante del documento de residencia una idea completa de todos esos datos en forma inteligible, es decir, permitiéndole conocer esos datos y comprobar que son exactos y son tratados de conformidad con esta Directiva para que pueda, en su caso, ejercer los derechos que los artículos 12, letras b) y c), 14, 22 y 23 de dicha Directiva le confieren.[63]

Con base en estos y otros varios considerandos, dicho TJUE resolvió de forma meridianamente clara que:

> El artículo 12, letra a), de la Directiva 95/46 y el artículo 8, apartado 2, de la Carta de los Derechos Fundamentales de la Unión Europea deben interpretarse en el sentido de que el solicitante de un documento de residencia dispone de un derecho de acceso a todos los datos personales que le conciernan que sean objeto de tratamiento por las autoridades administrativas nacionales en el sentido del artículo 2, letra b), de dicha Directiva. Para dar cumplimiento a este derecho, basta con facilitar a dicho solicitante una idea completa de esos datos en forma inteligible, es decir, permitiéndole conocer dichos datos y comprobar que son exactos y son tratados de conformidad con esta Directiva para que pueda, en su caso, ejercer los derechos que dicha Directiva le confiere.[64]

Conforme a lo anterior, es indudable que no existen criterios uniformes sobre el alcance del derecho de acceso, donde algunas jurisdicciones han interpretado que la puesta a disposición de una idea completa de esos datos en forma inteligible es suficiente para satisfacer la solicitud de acceso.

---

63 Tribunal de Justicia de la Unión Europea. Tercera Sala. Asuntos Acumulados C-141/12 y C-372/12. Recuperados de: *http://curia.europa.eu/juris/document/document.jsf?docid=155114&doclang=ES*

64 Ídem.

Derecho de rectificación

Los titulares de datos personales tienen derecho a rectificarlos cuando sean inexactos o incompletos.

Este derecho se puede ejercer de forma independiente a cualquiera de los demás derechos ARCO, cuando el propio titular sabe que sus datos son inexactos o están incompletos y desea actualizarlos o completarlos frente a un responsable específico o ejercido como consecuencia de un derecho previo de acceso, cuando el titular tiene conocimiento de que los datos en posesión del responsable no son exactos o no están completos.

Como requisito específico para el ejercicio del derecho de rectificación, el artículo 104 del Reglamento de la LFPDPPP prevé que el titular deberá acompañar la documentación que ampare la procedencia de la actualización o corrección respectiva, si bien es cierto que el propio numeral también establece que el responsable podrá ofrecer mecanismos que faciliten el ejercicio de este derecho en beneficio del titular.

En la práctica, el ejercicio de este derecho puede ocurrir (y ha ocurrido incluso antes de la entrada en vigor de la LFPDPPP) mediante solicitudes informales (por ejemplo, vía telefónica o presencial) que efectivamente facilitan a los titulares la actualización o corrección de sus datos; como en todos los casos, será el propio responsable quien deberá determinar los medios más convenientes para facilitar el ejercicio de este derecho, sin descontar, en ningún momento, el uso de medios electrónicos previa identificación y autenticación del titular.

En consonancia con lo dispuesto en el artículo 25 de la LFPDPPP, el INAI recuerda que el derecho de rectificación no se limita, en su caso, a la información en posesión del responsable requerido, sino que puede alcanzar a terceros a los que se hayan transferidos datos del titular:

> Si la información personal a rectificar ha sido transferida a terceros nacionales o extranjeros con anterioridad, el responsable debe informar a éstos de tal situación para que procedan a efectuar la corrección correspondiente.[65]

A través de la guía en cita, el INAI no hace sino recalcar que los responsables deben establecer procesos que permitan la trazabilidad de los datos personales bajo su responsabilidad, de manera que éstos siempre puedan referirse a los terceros a los cuales hayan transferido datos personales para que efectúen correcciones o actualizaciones solicitadas por sus titulares.

[65] IFAI. (2011). Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO, p.8.

Derecho de cancelación

Para comprender el alcance del derecho de cancelación debemos tener presente, en primer lugar, la definición de un concepto intrínsecamente asociado a este derecho: el bloqueo. El artículo 3, fracción III de la LFPDPPP establece que por tal deberemos entender:

La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.

El INAI explica el propósito del bloqueo de la siguiente forma:

> El propósito del bloqueo es resguardar los datos por un tiempo razonable en el que podrían surgir responsabilidades relacionadas con el tratamiento, esto es, responsabilidades que para poder ser verificadas, requieran de los datos personales del titular. Durante este periodo, los datos no podrán ser tratados para otra finalidad.[66]

Como referencia organizativa, y en congruencia con el artículo 3, fracción III de la LFPDPPP, todo responsable debe recordar que conforme al último párrafo del artículo 108 del Reglamento de la LFPDPPP, el período de bloqueo será el plazo de prescripción legal o contractual correspondiente. Por lo anterior, es indispensable la identificación de todos los datos personales objeto de tratamiento, su fecha y medio de obtención, así como las finalidades por los cuales resulta necesario u obligatorio su tratamiento.

Luego entonces, si la solicitud de cancelación de datos personales resulta procedente, el responsable requerido para efectuarla deberá proceder al bloqueo de los datos identificados por el titular, tras lo cual deberá suprimir de forma definitiva la información. Cuando la cancelación se haya efectuado en su totalidad, el responsable deberá dar aviso al titular.

Adicionalmente, como titulares y como responsable de datos personales, debemos saber que el artículo 106 del Reglamento de la LFPDPPP dispone que los titulares podrán solicitar la cancelación de sus datos en todo momento y cuando consideren que no están siendo tratados conforme a los principios y deberes que establece la normativa, y que la cancelación se puede solicitar

[66] Ídem, p. 9.

sobre la totalidad de los datos contenidos en una base de datos, o sólo sobre una parte de ellos.

Es importante tener en cuenta que las medidas de trazabilidad de los datos personales que deben ser implementadas por los responsables explican, en su justa medida, lo dispuesto por el cuarto párrafo del artículo 25 de la LFPDPPP:

> Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también.

En todo caso, debemos considerar que el derecho a la cancelación de datos no es un derecho absoluto, ya que existen diversos supuestos (previstos de forma taxativa en el artículo 26 de la LFPDPPP) que facultan al responsable para negar la cancelación de datos personales referidos en una solicitud específica.

Asimismo, y tal y como ocurre con cualquier otra respuesta al ejercicio de los derechos ARCO, si el titular no está satisfecho con la negativa del responsable a la cancelación de sus datos, podrá acudir al INAI para que dentro de un procedimiento de protección de derechos se resuelva la procedencia o improcedencia de dicha negativa.[67]

Finalmente, resulta sumamente útil para los responsables atender a las recomendaciones organizativas que el INAI ha difundido para que adopten las acciones necesarias cuando resulte procedente una solicitud de cancelación de datos personales:

1. Determinar el periodo de bloqueo de la información personal, notificando el mismo en la respuesta que le dé al titular sobre su solicitud de cancelación.
2. Realizar operativamente el bloqueo de los datos personales.
3. Implementar las medidas de seguridad que permitan conservar los datos personales, deshabilitando cualquier explotación de la información.
4. Dar aviso a los encargados del tratamiento de los datos personales a quienes se les hubiere comunicado los datos, a efecto de que procedan a la supresión respectiva.
5. Suprimir los datos personales correspondientes de tal manera que la eliminación no permita la recuperación de la información bajo ninguna técnica, transcurrido el periodo de bloqueo.[68]

---

67 Cfr. Reglamento de la LFPDPPP, capítulo VIII.

68 IFAI. (2011). *Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO*, p. 9.

Derecho de oposición

El derecho de oposición al tratamiento de datos personales ha dado lugar a diversas interpretaciones y, en no pocas ocasiones, se confunde en su naturaleza y alcance con el derecho de cancelación.

Encontramos que el INAI ha desarrollado una explicación sencilla sobre este derecho, que en la presente obra vale la pena mencionar:

> Es el derecho que tienes de solicitar que tus datos personales no se utilicen para ciertos fines, o de requerir que se concluya el uso de los mismos a fin de evitar un daño a tu persona. También en este caso, como en el anterior, no siempre se podrá impedir el uso de tus datos personales, cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.[69]

En este sentido, el derecho de oposición no conlleva la cancelación de los datos en posesión del responsable ante el que se ejerce, sino la solicitud para que dejen de ser utilizados para finalidades específicas que no resultan necesarias para el cumplimiento de disposiciones legales o para el cumplimiento de una relación jurídica.

Desde la entrada en vigor de la LFPDPPP, el derecho de oposición se ha asociado de forma cotidiana a la facultad de los titulares para solicitar a los responsables que dejen de tratar sus datos para fines mercadotécnicos o publicitarios, con el objeto de evitar seguir recibiendo publicidad electrónica, telefónica o postal del responsable, y sin que ello conlleve la terminación de la relación jurídica principal. "Así, el derecho de oposición, mantiene a salvo otros fines del tratamiento que el responsable, de conformidad con su aviso de privacidad, puede llevar a cabo y con los que el titular está de acuerdo".[70]

Lo anterior no resulta extraño si tomamos en cuenta que en el artículo 110 del Reglamento de la LFPDPPP se regula de manera expresa la gestión de listados de exclusión, a través de los cuales se podrán incluir a las personas que han manifestado su negativa para el tratamiento de sus datos personales, en relación con "los productos" del responsable o de terceras personas.

Asimismo, recordemos que el artículo 111 del Reglamento se refiere a los registros públicos de consumidores y usuarios e indica que seguirán vigentes sin perjuicio de las disposiciones de la LFPDPPP y su reglamento, y que se regirán de conformidad con sus propias leyes y disposiciones aplicables que de aquellas se deriven.

---

[69] INAI. (2017). *Guía para titulares de los datos personales*. Vol. 3, p. 7.
[70] IFAI. (2011). *Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO*, p. 9.

Sin perjuicio de lo anterior, el derecho de oposición también resulta procedente en casos en que el responsable lleve a cabo un tratamiento de los datos personales de forma lícita, apegada a todos los principios establecidos por la LFPDPPP, y sin embargo, la persistencia del tratamiento puede ocasionar un perjuicio a un titular que cuenta con una razón legítima derivada de su propia situación personal que lo faculta para oponerse a la continuidad del tratamiento de sus datos para fines específicos.

En estos casos, la solicitud de oposición al tratamiento de datos puede constituirse en un ejercicio complejo, que requerirá de la exposición y prueba de:

- La causa legítima y la situación específica del titular que justifica la solicitud de oposición a pesar de la licitud del tratamiento efectuado por el responsable.
- El perjuicio que causa al titular el tratamiento de sus datos.
- Las razones por las que la persistencia del tratamiento concreto causa ese perjuicio.
- Las razones por las cuales el cese del tratamiento traerá como consecuencia el propio cese del perjuicio.

Sin duda, el ejercicio del derecho de oposición en los términos antes indicados deberá construirse a partir de razones y situaciones específicas, sustentadas en pruebas y determinados criterios objetivos y subjetivos, y su resultado no será del todo previsible en todos los casos, pudiendo llegar a ser el propio INAI quien deba valorar la procedencia de solicitudes específicas al respecto:

> En caso de que el derecho de oposición sea ejercido debido a que le causa un perjuicio al titular, éste, en su solicitud, deberá explicar el perjuicio que, en su caso, le ocasione el tratamiento de los mismos a fin de que el responsable, y en su caso el Instituto, puedan hacer una valoración sobre si este derecho puede o no ser llevado a cabo.[71]

Desde luego, y tal y como ocurre con cualquier otro de los derechos ARCO que hemos analizado, no debemos descartar que el Poder Judicial de la Federación deba ser el encargado final de resolver o interpretar el alcance del derecho de oposición por causas de perjuicio al titular de los datos. Sin embargo, y hasta la fecha de publicación de esta obra, no existen tesis ni jurisprudencias sobre el alcance, contenido o limitaciones de este derecho, ni de ningún otro de los derechos ARCO.

[71] Íbid, p.10

Decisiones sin intervención humana valorativa

De suma relevancia para el presente y el futuro de la protección de datos personales y otros derechos y libertades de los ciudadanos, pero aún alejado del nivel de cumplimiento e importancia otorgado a otras disposiciones de nuestra normativa, el artículo 112 del Reglamento de la LFPDPPP constituye el primer intento del legislador mexicano para reconocer derechos a los titulares cuando existen decisiones automatizadas que afectan a su esfera jurídica, adoptadas precisamente a partir del tratamiento de sus datos personales.

La relación de los derechos ARCO con este tipo de decisiones se explica en el segundo párrafo del artículo de referencia, el cual mencionaremos más adelante.

La comprensión de las disposiciones del artículo 112 del Reglamento de la LFPDPPP supone reconocer que existen tratamientos automatizados (sin intervención humana) de datos personales, cuya finalidad es la toma de "decisiones" que puedan afectar a las personas físicas, y supone el conocimiento de sus disposiciones:

> Artículo 112. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre.
> Asimismo, el titular podrá ejercer su derecho de acceso, a fin de conocer los datos personales que se utilizaron como parte de la toma de decisión correspondiente y, de ser el caso, el derecho de rectificación, cuando considere que alguno de los datos personales utilizados sea inexacto o incompleto, para que, de acuerdo con los mecanismos que el responsable tenga implementados para tal fin, esté en posibilidad de solicitar la reconsideración de la decisión tomada.

Estos tratamientos son cada vez más comunes y afectan de diversas formas a la esfera jurídica de aquellas personas que han sido objeto de una valoración en la que no intervino un ser humano. Llegados a este punto, el lector ya habrá deducido que hablamos del uso de algoritmos[72] que, alimentados con datos de personas físicas, procesan esta información para emitir resultados (decisiones) con mayor o menor relevancia para aquellos que fueron objeto de la valoración.

A manera de ejemplo, podemos citar dos tratamientos algorítmicos relativamente comunes en el año 2018: (i) la solicitud en línea de créditos al consumo y (ii) el tratamiento de datos de candidatos a puestos de trabajo.

[72] La Real Academia de la Lengua Española (RAE) define algoritmo (primera acepción) como el "conjunto ordenado y finito de operaciones que permite hallar la solución de un problema". RAE. (2017). *Diccionario de la Lengua Española en línea*, concepto de "algoritmo". Recuperado de: *http://dle.rae.es/?id=1nmLT*sh

En el primer ejemplo, y de manera general, el tratamiento de los datos personales ocurre a partir de que el titular accede a vincular su perfil de cualquier red social, como requisito previo e indispensable para solicitar una valoración de su persona como sujeto de crédito. Esta vinculación conlleva el acceso de un algoritmo a todos los datos personales y resto de información disponible en el perfil de la persona que solicita el crédito. El algoritmo analizará la información a la que se le ha concedido acceso y, en cuestión de segundos, a partir de su propia programación, emitirá una decisión binaria: sí o no, para determinar si el solicitante es o no sujeto de crédito.

La explicación del segundo ejemplo es relativamente sencilla, en la medida en que, a partir de parámetros relativamente sencillos, cualquier programa (algoritmo) puede desechar de un proceso de selección laboral a cualquier persona cuyos datos personales conformen un perfil no deseado por la organización que ha convocado ese proceso. Este tratamiento no conlleva por sí mismo un ejercicio ilegal por discriminatorio, dado que puede estar basado en el interés legítimo de la organización para incluir en sus procesos de selección únicamente a personas que vivan cerca de sus instalaciones o que reúnan determinados estudios indispensables para el desempeño del puesto, pero, como en el ejemplo anterior, no significa que por esta razón los derechos de los titulares deban ser ignorados.

Para comprender los derechos a favor de las personas que son objeto de una “decisión sin intervención humana valorativa”, debemos identificar que el primer derecho regulado por el artículo 112 de referencia es el de información, disponiendo que ante la existencia de un tratamiento de datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, los responsables deberán informar de esta situación a los titulares de los datos. Evidentemente, esta información deberá proporcionarse a través del aviso de privacidad correspondiente.

Pero en adición al derecho de información antes indicado, en el segundo párrafo del artículo 112 se reconoce de manera expresa que en estas situaciones los titulares tienen derecho de acceso para “conocer los datos personales que se utilizaron como parte de la toma de decisión correspondiente” y, en su caso, el derecho de rectificación, “cuando considere que alguno de los datos personales utilizados (en el proceso de toma de decisiones) sea inexacto o incompleto”.

Como nota relevante, merece nuestra atención la mención (¿reconocimiento?) a un derecho que sólo encontraremos referido en este artículo: el derecho a la reconsideración de la decisión adoptada en el proceso de toma de decisiones, cuando ésta se basó en datos personales inexactos o incompletos.

No debemos pasar por alto que los derechos de acceso, rectificación y reconsideración antes indicados no conceden a los titulares ningún tipo de derecho para conocer la forma en que el algoritmo funciona, ni los criterios que dicho medio automatizado utiliza para arribar a una "decisión sin intervención humana valorativa", estos derechos se limitarán a los datos personales del titular valorado.

Todo lo anterior pone de manifiesto la importancia del derecho de información vinculado con el derecho para el ejercicio de los derechos ARCO, cuando en situaciones tan específicas como la anterior, los titulares tienen derecho a acceder a sus datos usados para adoptar una decisión automatizada, y su derecho para rectificar aquéllos que pudieran no estar correctos o actualizados. Sin duda, estos son derechos que cualquier persona tendrá facultad de ejercer frente al uso de algoritmos, *big data* o inteligencia artificial para el tratamiento de sus datos personales.

Conclusiones

Desde su publicación y entrada en vigor, la LFPDPPP ha supuesto un hito en la regulación y protección de un derecho hasta entonces poco reconocido en nuestro país: la protección de los datos de las personas físicas.

Como parte fundamental de dicho derecho, los conocidos como "derechos ARCO" se constituyen en auténticos pilares de dicha protección y de la autodeterminación informativa que todo individuo tiene derecho a ejercer frente a cualquier responsable en posesión de sus datos.

En su aspecto más público, la existencia de los derechos ARCO ha supuesto un cambio de paradigma en la relación de las personas con los responsables que tratan sus datos, forman parte de la creciente cultura de la protección de datos personales que se desarrolla en nuestro país, y sólo cabe esperar que cada vez más ciudadanos ejerzan estos derechos de manera normal y cotidiana.

Para respetar su ejercicio, todo responsable debe emprender acciones de cumplimiento al interior de su organización, que van más allá de la simple publicación de avisos de privacidad que declaren la existencia de medios para ejercerlos, es necesario que existan personas o departamentos encargados de su gestión para que cualquier persona reciba respuesta a una solicitud de derechos ARCO y, evidentemente, para evitar que los responsables incurran en responsabilidad administrativa como resultado de una gestión inadecuada de las mismas.

Finalmente, y frente al creciente uso de tecnologías de inteligencia artificial, es necesario que los responsables que aprovechan sus ventajas sean conscientes de las responsabilidades inherentes a su uso en relación con el tratamiento de datos personales y de los efectos que pueden tener sobre las personas cuando se utilizan para la toma de decisiones. En estos escenarios, el respeto de los derechos de información, acceso, rectificación y reconsideración debe ser una prioridad para todo responsable que se ubique en los supuestos que regula el artículo 122 del Reglamento de la LFPDPPP.

Referencias

AEPD. Portal oficial de la Agencia Española de Protección de Datos. Recuperado de: *https://www.aepd.es/*

_____. (2018). *Guía para el ciudadano*. Recuperado de: *https://www.aepd.es/media/guias/guia-ciudadano.pdf*

Consejo de Europa. (1981). *Convenio para protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.* Recuperado de: *https://rm.coe.int/16806c1abd*

Directiva 95/46/CE del Parlamento Europeo y del Consejo (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.* Recuperado de: *https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A31995L0046*

Asia-Pacific Economic Cooperation. (2005). *APEC Privacy Framework.* Recuperado de: *https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf*

IFAI. (2011). *Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO.* Recuperado de: *http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf*

INAI. (2017). *Guía para Titulares de los Datos Personales.* Vol. 3. Recuperado de: *http://corpusiurispdp.inai.org.mx/iberoamericano/OtrosDocumentos/Guia%20Titulares-03_PDF.pdf#search=ARCO*

____. (2017) *Guía para Titulares de los Datos Personales*. Volumen 3. Recuperado de: *http://corpusiurispdp.inai.org.mx/iberoamericano/OtrosDocumentos/Guia%20Titulares-03_PDF.pdf#search=ARCO*

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). Recuperado de: *https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32016R0679*

Organización para la Cooperación y el Desarrollo Económicos. (2013). *Directrices sobre protección de la privacidad y flujos transfronterizos*

de datos personales. Recuperado de: *http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm*

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), *https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32016R0679*

Tribunal de Justicia de la Unión Europea. Tercera Sala. Asuntos Acumulados C-141/12 y C-372/12 (Minister voor Immigratie, Integratie en Asiel). 2014. Recuperado de: *http://curia.europa.eu/juris/document/document.jsf?docid=155114&doclang=ES*

CAPÍTULO IV

DEL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

CAPÍTULO IV
DEL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

Artículo 28. *El titular o su representante legal podrán solicitar al responsable en cualquier momento el acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen.*

Artículo 29. *La solicitud de acceso, rectificación, cancelación u oposición deberá contener y acompañar lo siguiente:*

I. El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud;
II. Los documentos que acrediten la identidad o, en su caso, la representación legal del titular;
III. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y
IV. Cualquier otro elemento o documento que facilite la localización de los datos personales.

Artículo 30. *Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la presente Ley. Asimismo fomentará la protección de datos personales al interior de la organización.*

Artículo 31. *En el caso de solicitudes de rectificación de datos personales, el titular deberá indicar, además de lo señalado en el artículo anterior de esta Ley, las modificaciones a realizarse y aportar la documentación que sustente su petición.*

Artículo 32. *El responsable comunicará al titular, en un plazo máximo de veinte días, contados desde la fecha en que se recibió la solicitud de acceso, recti-*

ficación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta. Tratándose de solicitudes de acceso a datos personales, procederá la entrega previa acreditación de la identidad del solicitante o representante legal, según corresponda.

Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Artículo 33. *La obligación de acceso a la información se dará por cumplida cuando se pongan a disposición del titular los datos personales; o bien, mediante la expedición de copias simples, documentos electrónicos o cualquier otro medio que determine el responsable en el aviso de privacidad.*

En el caso de que el titular solicite el acceso a los datos a una persona que presume es el responsable y ésta resulta no serlo, bastará con que así se le indique al titular por cualquiera de los medios a que se refiere el párrafo anterior, para tener por cumplida la solicitud.

Artículo 34. *El responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos:*

I. Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;
II. Cuando en su base de datos, no se encuentren los datos personales del solicitante;
III. Cuando se lesionen los derechos de un tercero;
IV. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y
V. Cuando la rectificación, cancelación u oposición haya sido previamente realizada.

La negativa a que se refiere este artículo podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular.

En todos los casos anteriores, el responsable deberá informar el motivo de su decisión y comunicarla al titular, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes.

Artículo 35. *La entrega de los datos personales será gratuita, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos.*

Dicho derecho se ejercerá por el titular en forma gratuita, previa acreditación de su identidad ante el responsable. No obstante, si la misma persona reitera su solicitud en un periodo menor a doce meses, los costos no serán mayores a tres días de Salario Mínimo General Vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas.

El titular podrá presentar una solicitud de protección de datos por la respuesta recibida o falta de respuesta del responsable, de conformidad con lo establecido en el siguiente Capítulo.

COMENTARIO

Guillermo A. Tenorio Cueto

Introducción

El presente comentario está relacionado con el capítulo 4 de la Ley de Protección de Datos Personales en Posesión de los Particulares, el cual versa sobre el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición).[73] Este ejercicio involucra, de manera determinante, no sólo al titular de los derechos como parte activa del mismo, sino al responsable del tratamiento de datos personales, el cual nos aparece como garante y ejecutor de la solicitud de protección de dichos derechos.

Los comentarios vertidos en este capítulo se encuentran propuestos a partir del enramado de políticas y procedimientos que el responsable deberá implementar de cara a la solicitud del titular del derecho, los cuales, sin una adecuada implementación de las medidas de seguridad administrativas, no podrán llevarse a cabo.

En efecto, el eje central de todo el comentario será justamente esas medidas de seguridad. Sin ellas de nada sirve el aviso de privacidad o la

[73] Es importante referir que la protección de datos personales es, en realidad, una debida protección al titular del derecho que se garantiza a través de la referencia constitucional de sus cuatro derechos que forman parte de la autodeterminación informativa como derecho conexo a la vida privada. Para mayor referencia ver: Davara, I. (2010). "Protección de datos de carácter personal en México: Problemática jurídica y estatus normativo actual". En *Protección de datos personales*. México. H. Cámara de diputados-IFAI-ITAM, p.78.

enumeración puntual de los derechos ARCO en el mismo aviso. Dichas medidas de seguridad responderán a un cumplimiento adecuado de las previsiones que, tanto la Ley como su reglamento contemplan. Así, ellas se constituirán en la piedra angular de un debido ejercicio de los derechos ARCO.

El presente análisis lo hemos dividido en diversos apartados que le permitirán al lector acercarse temáticamente a cada uno de los comentarios vertidos. Encontraremos subapartados vinculados a: a) identidad y representación, b) elementos para encontrar los datos personales de los titulares, c) envío y atención de la solicitud, d) resolución por parte del responsable, f) efectividad de la resolución del responsable, g) negativa de la solicitudes y h) gratuidad de las solicitudes.

Correlaciones

Respecto al ejercicio de los derechos, este capítulo está correlacionado con los artículos 87, 88, 89, 90 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107,108, 109, 110 111 y 112 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Análisis de contenido

Hablar del ejercicio de los derechos ARCO es hablar, no sólo de procedimientos vinculados al responsable del tratamiento, sino penetrar en su vida interna a partir del conocimiento de las medidas de seguridad administrativas, de las políticas y procedimientos.[74]

En efecto, cuando hablamos de que un titular acude a un responsable a ejercer alguno de los derechos, presuponemos que ha establecido una serie de medidas al seno de su organización que permitiría que dicha solicitud pudiera solventarse conforme a lo que refiere la ley, pero también, de acuerdo con una estructura previamente establecida dentro del responsable donde se han asignado funciones en determinados perfiles de puesto y donde se han instrumentado procedimientos que, internamente, pueden dar respuesta oportuna sobre el tratamiento. Sin ello, el ejercicio de estos derechos se desmoronaría. Inclusive, la implementación de dichos procedimientos supondrá el establecimiento de un sistema de gestión y seguridad en materia de datos personales donde a través de una serie de fases y pasos se propone a los responsables un camino deseable para la implementación de dichas

[74] "Pensar en seguridad es pensar en minimización de riesgos, para conocer el riesgo es importante entender no sólo la naturaleza del dato sino la naturaleza de los medios de almacenamiento de la información y sus vulnerabilidades propias" Solis, C. (2018). "Las medidas de seguridad en materia de protección de datos",en Tenorio, G. (Coord.). *La protección de datos en México. Revisión crítica de su garantía en el ordenamiento jurídico mexicano*. México. TFJA.

medidas de seguridad que tendrán como uno de sus objetos primordiales la implementación de los mecanismos de ejercicio de los derechos ARCO.

Identidad y representación

Una vez referido lo anterior, y destacado el medular papel que revisten las medidas de seguridad administrativas para poder llevar a cabo el ejercicio de los derechos, nos enfrentamos a la solicitud del derecho. En ese sentido la LFPDPPP refiere que será el titular o su representante legal quienes pueden solicitar el ejercicio de los derechos ARCO.[75] Esta previsión de la Ley es acotada y precisada en el Reglamento de la misma, al señalarnos que la identidad, tanto del titular como del representante, deberá ser acreditada mediante copia del documento de identificación y luego deberá ser exhibido para su cotejo.

Lo anterior nos lleva a suponer que el responsable, en todo momento, deberá solicitar el documento en original para cotejar la identidad y la veracidad del documento que el titular envió en copia, pero habrá que ser cauteloso con ello, pues de entender este proceso de esa manera nos conduciría a un camino engorroso, poco dinámico y no acorde a la realidad informática actual. En ese sentido el Reglamento abre la puerta para lograr la identificación del titular y del responsable mediante "los instrumentos electrónicos por medio de los cuales sea posible identificar fehacientemente al titular"[76] o bien "aquellos previamente establecidos por el responsable"[77] con lo cual el Reglamento permite establecer en las políticas y procedimientos internos del responsable, la posibilidad de conducir libremente el modo de identificación del titular y su representante para iniciar el procedimiento de ejercicio de los derechos ARCO.

A la par de lo anterior, la Ley no deja claro la acreditación del representante legal y tampoco es precisa respecto a la representación de los menores de edad. En ambos casos, el Reglamento nos da luces al establecer que la representación puede llevarse a cabo a través de los instrumentos públicos correspondientes o a través de una carta poder firmada ante dos testigos, lo que en ningún caso se aclara es si debe incluir la leyenda que específicamente se dota al representante para la tramitación del ejercicio de derechos ARCO. Desde nuestro particular punto de vista debería de referirse e incluirse.

En el caso de menores de edad, personas en estado de interdicción y personas con incapacidad, la respuesta no la encontramos en la Ley, sino en el Reglamento donde se hace mención a las reglas de representación dispuestas

[75] Artículo 28 de la LFPDPPP.
[76] Artículo 89 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante RLFPDPPP).
[77] Ídem.

en el Código Civil Federal.[78] En ese sentido, baste recordar que para efectos de menores de edad el ejercicio de los derechos ARCO estará a cargo de aquellos que ejercen la patria potestad. Para los casos en los cuales existe separación o divorcio habrá que atenderse si existió o no pérdida de la patria potestad de alguno de los padres, pues de lo contrario, el ejercicio de los derechos ARCO estará a merced de la autorización de ambos. Si existiera la pérdida de la patria potestad por alguno de ellos, será necesaria la acreditación del documento judicial que condena a dicha pérdida, de lo contrario el responsable no podrá llevar a cabo el ejercicio del derecho ARCO pues se entendería que ambos padres siguen ejerciéndola. Para el caso de terceros que pudieran ejercer la patria potestad respecto a un menor fuera de los padres, el responsable deberá igualmente solicitar la acreditación de la representación al tutor.

Elementos para encontrar los datos personales del titular

A la par de lo anteriormente descrito, la Ley ordena al titular del derecho que para el caso de la solicitud de los derechos ARCO es necesario describir con claridad y precisión "los datos personales respecto de los que se busca ejercer alguno de los derechos" o bien "acompañar cualquier otro elemento que facilite la localización de los datos personales"[79] lo cual en la práctica cotidiana puede generar diversos problemas. En efecto, cuando hablamos de datos personales vinculados con el derecho de rectificación se actualiza a la perfección este supuesto, pues el titular del derecho deberá remitir al responsable el o los datos que quiera rectificar y de qué manera se deberá efectuar dicha rectificación. Más no es así cuando hablamos del derecho de acceso, pues en este supuesto el titular del derecho sólo querrá saber qué datos se tienen de él, sin poder precisarle al responsable con claridad y exactitud los datos origen de la solicitud. En el caso del derecho de oposición, debemos hablar de finalidades del aviso de privacidad a las cuales nos oponemos por lo que esta descripción clara y precisa de la que habla la fracción III del artículo 29 de la Ley tampoco se actualiza en virtud de que el ejercicio de este derecho está referido, no a un dato en concreto, sino a la negativa de un tratamiento determinado vinculado a las finalidades propuestas por el responsable. En el caso de cancelación de datos, el titular deberá ser preciso, no sólo en el dato sino en el conjunto de datos que busca cancelar, por lo que en este supuesto la solicitud deberá ser precisa y clara respecto ellos.

Aquí sólo hemos hablado de datos muy concretos donde el titular del derecho fácilmente los reconoce, pero hoy los adelantos tecnológicos nos plantean retos sin precedentes donde luego de procesos de disociación en proyectos de *big data*, los datos vuelven a asociarse y generan perfiles muy definidos con tendencias de compra, perfiles políticos o bien revelando aspectos

[78] Para mayor abundamiento revisar los títulos octavo y noveno del Código Civil Federal.
[79] Artículo 29 de la LFPDPP.

clínicos en donde el titular del derecho podría exponer algún dato que otorgó pero que, sin lugar a dudas, no tendría idea de cómo ha sucedido un proceso de asociación respecto otros datos que el responsable ha adquirido y que ha potenciado la construcción de una información que puede afectar la vida más íntima de la persona.[80] En estos casos estamos desprovistos de precisar con claridad y exactitud los datos que los responsables tienen de nosotros.[81]

Envío y atención de la solicitud

Como adelantamos al inicio del presente comentario, el ejercicio de los derechos ARCO no podría llevarse a cabo si el responsable no cuenta previamente con las medidas de seguridad administrativas que establecen políticas y procedimientos de actuación para todo el personal de la organización que aparece como responsable. El artículo 30 de la Ley es enfático y consecuente en ello al referir que todo responsable debe designar a una persona o a un departamento de datos personales y fomentar, dentro de su organización, la protección de datos personales.[82] En ese entendido es importante destacar dos elementos primordiales:

a) que el procedimiento de ejercicio de los derechos ARCO esté contemplado en el aviso de privacidad y
b) que el responsable haya implementado el procedimiento necesario al seno de la organización para el debido ejercicio de los derechos ARCO.

Como podemos observar este ejercicio enfrenta al titular directamente con el responsable en dos momentos: al inicio de la elaboración de la solicitud, en donde el titular es informado de cómo llevar a cabo dicha solicitud, hacerla llegar al responsable y de qué manera será ejecutada en la organización.

---

80 Cfr. Morte, R. (2017). "¿Protección de datos/privacidad en la época del Big Data, IoT, wearables…?" Sí, más que nunca. *Dilemata,* revista internacional de ética aplicada. No. 24. pp. 219-233. En ese sentido el autor destaca cuatro grandes grupos de riesgo refiriendo que: "Las posibilidades que ofrece el tratamiento masivo de datos abre nuevas oportunidades en el mundo de la ciencia y de los negocios, pero presenta nuevos peligros en torno a un posible uso inadecuado de esos datos. Las aplicaciones de *big data* tienen como objetivo el prever posibles pautas de comportamiento de una persona o grupo de personas. Algunos ejemplos a) analizar la posibilidad de un comportamiento determinado en relación con diferentes tipos de contratos (*scoring*), b) acumular datos en principio inconexos con el fin de crear un perfil detallado de una persona o de un grupo de personas (*profiling*), c) valorar diferentes características de una persona, como pueden ser su estado de salud, sus gustos o su fiabilidad (*personalizing*) y d) seguir a una persona con base al rastro que deja, por ejemplo en internet (*tracking*)".

81 El convenio 108 del Consejo de Europa puede ser un punto de partida interesante respecto a los tratamientos automatizados de datos y al flujo transfronterizo en donde los proyectos de *big data* quedan insertados. México lo adoptó el 12 de junio de 2018.

82 Cfr. Remolina, N. (2013). "Los derechos de acceso, rectificación, cancelación y oposición en la Ley de datos personales y su reglamento", en Piñar, J. Ornelas, L. (coords.). *La protección de datos personales en México*. México. Tirant lo Blanch, p. 191.

En el primer momento asumimos que el aviso de privacidad, como documento informativo del tratamiento, deberá contemplar el procedimiento necesario para el ejercicio de los derechos ARCO.[83] Esto se traduce en la inclusión precisa y detallada del mecanismo a través del cual se pueden ejercer (un correo electrónico, una dirección con precisión de área y ventanilla a la cual se debe dirigir el titular o bien los formatos donde puede completar la solicitud del ejercicio de los derechos) y desde luego, la precisión de lo que ocurrirá una vez enviada la solicitud. Llama la atención cómo, en la práctica cotidiana, muchos avisos de privacidad no cuentan con esos elementos.

En el segundo momento hablamos del proceso interno de la organización para responder y llevar a buen puerto la solicitud del titular. En muchas ocasiones los responsables que implementan políticas y procedimientos al seno de sus organizaciones se preguntan sobre quién o quienes deben atender las solicitudes o cuántas personas deben componer el departamento o área de protección de datos. En realidad, ello dependerá de muchos factores y no se puede establecer una regla general. La ley sólo refiere, en su artículo 30, la importancia de que exista la persona o el área que procese adecuadamente la solicitud de derechos ARCO. Observamos que muchos responsables no procesan adecuadamente estas solicitudes porque no cuentan ni con políticas ni con procedimientos, o bien debido a que la designación de la persona o área ha sido realizada erróneamente, pues no tiene el alcance operativo para irradiar y comunicar los efectos de la solicitud.

Resolución por parte del responsable

La necesaria implementación de políticas de privacidad en el seno de los responsables de tratamiento de datos se vuelve uno de los asuntos medulares de este apartado de la Ley, pues como refiere el artículo 32 de la LFPDPPP: "El responsable comunicará al titular…la determinación adoptada…respecto a la solicitud de derechos ARCO que éste realice a aquél".[84] Es evidente que sin una adecuada implementación de las referidas políticas, sería imposible que el responsable contestara la solicitud del titular del derecho. En efecto, el responsable deberá dotar de facultades a todo su entramado organizacional y definir los perfiles y los atributos necesarios para el puesto de responder a las solicitudes.

---

83 En realidad, el aviso de privacidad colma el principio de información. Dicho principio "…es aquél por el que se garantiza que el titular de los datos personales conozca con precisión, claridad y de forma oportuna qué datos se tratarán, para qué serán tratados, por quién, por cuánto tiempo, si serán transferidos, cómo podrá oponerse a su tratamiento o revocar, en su caso, el consentimiento que sobre su tratamiento pudiera haber otorgado con anterioridad y cualquier otra particularidad relativa a su tratamiento". Rivero, M. *El principio de información en materia de protección de datos personales en México*, en Tenorio, *op. cit*., p. 62.

84 Artículo 32 de la LFPDPPP.

A la par de lo anterior, el responsable no sólo dotará de competencias o facultades a los diversos puestos que tratan datos personales en la organización, sino también deberá implementar procedimientos claros que le permitan hacer efectiva la solicitud, lo cual tiene diversas implicaciones como:

a) Confirmación de identidad del titular del derecho.
b) Estudio y procesamiento de la solicitud.
c) Comunicación interna de la resolución adoptada que impacte en todas las áreas de la organización.
d) Respuesta de la solicitud.
e) Verificación de cumplimiento y auditoría del proceso.

En efecto, la recepción de una solicitud de derechos ARCO obliga al responsable a establecer un mecanismo claro que verifique y compruebe la identidad del titular del derecho que reclama la protección de los mismos, para ello, el responsable, como ya lo habíamos comentado con anterioridad, deberá capacitar a su personal para tales efectos y comunicar al titular los medios y la forma en la que debe comprobar dicha identidad.

De igual manera, deberán existir en la organización procedimientos estables que permitan rastrear los datos y el motivo de la solicitud, estableciendo los procesos y mecanismos necesarios para afectarlos en términos de lo requerido por el titular del derecho. En ese sentido, suele ocurrir en la práctica cotidiana que los responsables pretendan colmar el ejercicio del derecho ARCO del titular en una sola base de datos de la organización, situación que es errónea pues debería impactar en todas aquellas bases de datos en donde se concretan los datos afectados por la solicitud del titular, produciendo la imposibilidad de un adecuado ejercicio de aquellos derechos. El deber del responsable en el procesamiento de la solicitud debe ser colmar el ejercicio del derecho ARCO en todos aquellos lugares donde se encuentre el dato del titular. Es por ello que los procesos del responsable deben abarcar a toda la organización a través de procesos de comunicación interna que les permita, a todas las áreas, tener conocimiento pleno de la resolución adoptada impidiendo una vulneración o una carencia del principio de calidad en el tratamiento.

Efectividad de la resolución del responsable

Con todo lo anterior señalado, el responsable deberá comunicar la respuesta a la solicitud promovida por el titular del derecho.[85] La Ley contempla dos momentos:

[85] Cfr. Remolina. *op. cit.*, p. 191.

a) La comunicación de la respuesta.
b) Hacer efectiva la respuesta.

El alcance de esta previsión de la Ley tiene como efectos que el responsable comunique:

a) La procedencia o no del derecho ARCO ejercido.
b) El proceso de ejecución y efectividad de la resolución tomada para el caso de que procediera el derecho ARCO.
c) La temporalidad de ejecución.

En ese tenor, el responsable envía una comunicación que otorga certidumbre al titular sobre la protección de sus datos y que colma todos los principios en la materia. En esta respuesta encontramos, de alguna u otra manera, la concreción de todos y cada uno de dichos principios orientadores que buscan que el tratamiento sea el adecuado.[86] Desde luego, la efectividad de la respuesta, enunciación del procedimiento y la temporalidad de la ejecución de la misma se vería trunca si el responsable no cuenta con procesos de auditoría interna que permitan la supervisión, verificación y mejora de los procedimientos internos que garantizan el ejercicio de estos derechos.

Es claro que la respuesta a estas solicitudes abarcará diversas posibilidades de acuerdo con los diversos derechos ARCO que se promuevan. Así, es imperante saber que el tipo de respuesta estará motivada para el responsable si la solicitud versa sobre:

a) Derecho de acceso.
b) Derecho de rectificación.
c) Derecho de oposición.
d) Derecho de cancelación.

Cuando hablamos del derecho de acceso la Ley, tanto en su artículo 32 como en el 33 refiere, claramente, a que el cumplimiento de dicha obligación se tendrá por agotado cuando se entregue el o los datos requeridos en los términos que el responsable determine en el aviso de privacidad. Para el caso del derecho de acceso esta entrega podrá hacerse en los términos y medios que sean necesarios para el adecuado cumplimiento, siendo que, para el caso de requerir fijar los datos en soportes físicos o electrónicos, el responsable podrá cobrar su importe en términos de lo dispuesto por el artículo 35 de la misma ley.

[86] Baste recordar, como refiere Lucas, que el derecho a la autodeterminación informativa se colma no sólo del consentimiento y los llamados derechos de acceso, rectificación, cancelación y oposición, sino "…como es natural, a estas facultades de los titulares de los datos personales corresponden los relativos deberes de quienes los acopian, tratan, transmiten, conservan o utilizan de cualquier manera". Cfr. Lucas. P. (2008). "El derecho a la autodeterminación informativa y la protección de datos personales". *Cuadernos de derecho*. Azpilcueta. España. No. 20., p. 49.

Para el caso de derecho de rectificación, la respuesta y resolución estará sujeta a la solicitud misma y a los documentos o medios probatorios que envíe el titular del derecho para llevar a cabo dicha rectificación, tal y como se establece en el artículo 103 del Reglamento de la Ley.[87] Es claro que en la solicitud el titular del derecho indicará al responsable qué dato se encuentra inexacto y, desde luego, la corrección al mismo. Así por ejemplo, entenderemos que para efectos de datos de identificación, como podrían ser el domicilio, el teléfono, la CURP o el RFC, entre otros, será necesario que la solicitud venga acompañada del medio probatorio que avale dicho cambio. En ese sentido el responsable deberá incluir en sus procedimientos todos y cada uno de los documentos probatorios que pudieran contemplarse respecto a la rectificación de los datos. La respuesta por parte del responsable deberá estar orientada a:

a) Detallar el procedimiento de rectificación avalando los documentos probatorios anexados a la solicitud, mismo que se haría efectivo a los 15 días hábiles siguientes.
b) Requerir al solicitante de una mayor precisión respecto a los datos que requiere rectificar o bien respecto a los documentos que pudiera pedir para corroborar la veracidad de la nueva información.
c) Negar la solicitud e informar al titular el mecanismo ante la autoridad correspondiente para iniciar un procedimiento de protección de datos.

Para el caso del derecho a oposición, es importante destacar que la respuesta a la solicitud tendría los siguientes efectos:

a) Negar la solicitud en virtud del cumplimiento, por parte del responsable, de una obligación legal impuesta al responsable en virtud del artículo 109 del Reglamento.
b) Acceder a la oposición en virtud de tratarse de una finalidad secundaria del tratamiento de datos haciendo efectivo el traslado de los datos a la lista de exclusión a los 15 días hábiles luego de la respuesta al titular del derecho.
c) Acceder a la oposición derivado de una causa legítima que justifique el titular del derecho. Dicha causa deberá entenderse perjudicial para el titular y deberá ser evaluada por el responsable. Luego de la comunicación de la resolución se debe ejecutar la efectividad a los 15 días hábiles.
d) Negar la solicitud e informar al titular su derecho a iniciar un procedimiento de protección de datos ante la autoridad.

[87] Bien sabemos que como dice Nelson Remolina "…la rectificación está enfocada a controlar la calidad de la información de manera que se enmienden las imperfecciones, errores o defectos de la misma". Cfr. Remolina, *op. cit.*, p. 193.

Es importante referir, en el caso del derecho de oposición, que la solicitud no sólo podrá estar orientada a una finalidad en específico sino a una parte del tratamiento. Ello es trascendente, pues, por ejemplo, un titular podría oponerse a que se realicen transferencias de datos que no condicionen legalmente al responsable o bien que, al condicionarlo, dicha transferencia pudiera representarle un perjuicio serio. En todos los casos, los alcances del ejercicio deberán impregnar a toda la organización del responsable, a efecto de no generar una vulneración adicional luego de la efectividad de la solicitud. Es imperante recordar que la oposición no implica la cancelación.

De igual manera, para el caso de la efectividad del derecho de oposición, es necesario que el responsable forme una lista de exclusión. Dicha lista no supone una supresión de los datos, por el contrario, significa una oportunidad de tratamiento de datos en donde determinadas finalidades o tratamientos quedan excluidas del mismo. Todo responsable deberá crear un listado para finalidades y transferencias secundarias, y lo más importante, deberá otorgar al titular del derecho una constancia de su inscripción a la misma, la cual deberá notificarse al momento de hacerlo efectivo.

Para el caso del derecho de cancelación, la respuesta del titular adquirirá diversos caminos.[88] Sabemos que la cancelación de los datos implica, en términos del artículo 105 del Reglamento, el cese del tratamiento de los datos y luego de un periodo de bloqueo, la supresión de los mismos. Los caminos que abre este derecho para la respuesta del responsable son los siguientes:

a) Una relación jurídica existente entre el titular y el responsable.
b) Inexistencia de una relación jurídica entre el titular y el responsable.
c) Existencia de una relación jurídica que ya terminó.

Estas tres vías son de medular conocimiento para el responsable, pues de acuerdo con cada una de ellas, se procederá a efectuar la respuesta de la solicitud. El primer caso nos plantea la existencia de una relación jurídica. En ese sentido es necesario referir que la respuesta a la solicitud de cancelación de datos deberá ser una negativa, es decir, no procede la cancelación de datos personales cuando existe una relación jurídica viva, floreciente y activa. La petición de cancelación de datos se percibe, incluso, como un abuso por parte del titular para incumplir con sus obligaciones derivadas de dicha relación.

En el segundo supuesto encontramos el caso de la inexistencia de una relación jurídica entre el titular y el responsable, en este caso en concreto, los

[88] "Nótese que la cancelación tiene dos connotaciones; la primera como derecho del titular y la segunda como obligación del responsable del tratamiento. Sobre esta segunda acepción se observa como la cancelación guarda relación con el principio de finalidad del tratamiento de los datos y le corresponde al titular proceder a realizar la misma oficiosamente". Cfr. Ídem., p. 195.

efectos de la respuesta a la solicitud de cancelación serán los siguientes:

a) Acceder a la cancelación e indicar al titular el procedimiento a seguir para su efectividad, informándole sobre el periodo de bloqueo.
b) Solicitar una mayor información sobre los datos a cancelar.
c) Negar la cancelación.

La aceptación de la cancelación tiene como consecuencia directa el llamado periodo de bloqueo y la consecuente supresión del dato. La respuesta del responsable deberá detallar que el dato o los datos del titular susceptibles de ser cancelados serán enviados a una lista y permanecerán en ese estatus durante un determinado tiempo. Para el caso que examinamos, que supone la inexistencia de una relación jurídica, el periodo de bloqueo estará determinado por las políticas y procedimientos de la organización. En ese tenor, el periodo de bloqueo debe ser notificado al titular del derecho refiriendo, con total precisión que luego de vencido el dato o los datos, serán suprimidos de manera radical. De igual manera se debe precisar en la respuesta que, durante ese periodo, los datos ya no serán tratados para ninguna otra finalidad. En realidad, a partir de la efectividad de la respuesta por parte del responsable los datos no pueden ser afectados de ninguna manera.

El tercero de los supuestos que contemplamos es que existió entre el responsable y el titular una relación jurídica y que, con motivo de su terminación, el titular solicita la cancelación de los datos. En ese sentido es preciso que la respuesta por parte del responsable refiera:

a) Procedencia de la cancelación e inicio del periodo de bloqueo en términos del artículo 107 fracción I del Reglamento, en donde el responsable observará los plazos de prescripción de las acciones derivadas de la relación jurídica y que le imposibilitaría la eliminación del dato por ese periodo.
b) Negativa de la cancelación.

En el caso de la procedencia es imperante referir que el periodo de bloqueo no está determinado por las políticas o procedimientos, sino por los tiempos de prescripción de las acciones relativas o vinculadas a la relación jurídica. Durante este periodo el responsable no deberá tratar los datos del titular y sólo deberá esperar los plazos referidos para la supresión de la información en términos del Reglamento en su artículo 107 fracción IV.

Es imperante recordar que en el caso de periodo de bloqueo hablamos de que el único tratamiento posible es el de almacenamiento o el de acceso por alguna persona facultada por el responsable para efectos de la supresión.

Negativa de las solicitudes

Los derechos ARCO, como sucede con cualquier otro derecho o libertad, no se presentan como derechos absolutos, por el contrario, encuentran límites y en el caso que nos ocupa esos límites los encontramos en el primer momento del ejercicio de ellos mismos.[89] Así, el responsable puede negar el acceso, la rectificación, la cancelación y la oposición, siempre y cuando se presenten los supuestos en términos del artículo 34 de la Ley.

En ese sentido, la indebida acreditación del representante legal o bien que el pretendido titular en realidad no lo sea, motivará la respuesta por parte del responsable negando cualquiera de los derechos ARCO. En efecto, la carencia de identidad, o la falta probatoria de dicha identidad motivará la negativa. Para ello, la respuesta del responsable deberá estar orientada, previamente, a una especie de apercibimiento, en donde el responsable le refiera al pretendido titular o a su representante la carencia de documentos probatorios para que, en un plazo que el mismo responsable prevea en sus procedimientos, pueda ser subsanada por el titular. De lo contrario, la negativa se tendrá por firme.

Uno de los casos más típicos que pueden ocurrir es que el posible responsable no cuente con los datos del titular. Para ello, la respuesta a ese estatus durante un determinado tiempo deberá expresar, de manera fehaciente, la imposibilidad de dar cabida al ejercicio del derecho ARCO por la insuficiencia material de colmarlo por la falta de dichos datos. Esto puede deberse a tres posibilidades, que el responsable:

a) No tenga los datos.
b) No encuentre los datos.
c) Haya eliminado los datos.

El primer supuesto nos conduce directamente a la negativa. El segundo supuesto puede originarse a partir de la carencia de políticas y procedimientos para el tratamiento de datos por lo que el responsable, al comunicar la negativa, abre el camino para que el titular acuda a la autoridad garante a iniciar un procedimiento de protección de datos. Para el tercer supuesto el responsable responderá de manera expresa la negativa aclarando que los datos han sido suprimidos derivado de un proceso de eliminación interno o de la culminación de la temporalidad de la prescripción de las acciones legales correspondientes.

Una alternativa adicional a la negativa por parte del responsable se suscitará cuando exista algún tipo de impedimento, ya sea legal o resolutivo, de alguna autoridad que pueda restringir la posibilidad del ejercicio de los

[89] Cfr. Remolina. Ídem., p. 192.

derechos ARCO. En ese sentido, el responsable en su respuesta deberá negar la solicitud haciendo énfasis en el impedimento legal para hacerlo. Un claro ejemplo lo encontramos en los casos de pérdida de la patria potestad por parte de algún progenitor el cual se acerca al centro educativo del hijo para solicitar informes sobre las actividades, calificaciones o cualquier otro dato del menor. El centro educativo responderá la solicitud con una negativa por el impedimento que tiene de manera manifiesta.

La última posibilidad de negativa estará vinculada a una actividad de repetición del mismo derecho sobre el mismo dato. Esto tiene alcances interesantes, pues la Ley no hace distinción en su artículo 34 fracción V donde sólo habla de que existirá la negativa si el ejercicio del derecho ha sido previamente realizado. Esto en definitiva es un error de la Ley, pues es necesario precisar que, por ejemplo, en el derecho de rectificación la negativa estará presente cuando el titular del derecho lo ejerza en un tiempo menor de doce meses sobre el mismo dato, pero ello no obsta a que pueda ejercer el mismo derecho de rectificación sobre otro dato, con lo cual, el responsable no deberá emitir una negativa al respecto.

Lo mismo ocurrirá con la oposición y la cancelación. En ambos casos el ejercicio del derecho deberá negarse cuando el titular lo pretenda respecto de la misma información que ya ha sido cancelada o sobre la finalidad que ya ha sido causa de oposición. Es claro que, en estos casos, la respuesta del responsable será la negativa, no así cuando el titular busque oponerse a otra finalidad, otra transferencia u otra fase de tratamiento o bien cuando habiendo solicitado la cancelación de algún dato en manos del responsable busque la supresión de algún otro. En estos últimos supuestos la negativa no sería una opción siendo que el responsable deberá garantizar un adecuado ejercicio del derecho en cuestión.

Gratuidad de las solicitudes

Sin lugar a dudas, uno de los temas polémicos del ejercicio de los derechos ARCO es el tema de la gratuidad de las solicitudes contenida en el artículo 35 de la Ley. Para entender el tema es necesario hacer algunas distinciones. La primera de ella es que podemos decir que por regla general se entiende que las solicitudes en materia de protección de datos ante el responsable son gratuitas,[90] pero como suele suceder con toda regla general existen dos excepciones. Las cuales son:

a) El costo de reproducción en algún material u otro formato.
b) La petición reiterada.

[90] Así lo entiende también Nelson Remolina, quien refiere que "…el ejercicio de los derechos ARCO debe ser sencillo y parcialmente gratuito. El titular debe cubrir algunos costos… pero el monto tiene limitaciones…" Cfr. Remolina. Ídem., p. 191.

En el primer supuesto el responsable deberá incorporar en la respuesta la leyenda que la entrega de datos (para el caso de acceso que se contemple en algún soporte material específico) tendrá un costo dependiendo de dónde se fije la información. Dicho costo será absorbido por el titular previamente a la entrega de los datos.

El segundo supuesto es interesante, pues la Ley no hace distinción sobre lo que llamamos la petición reiterada, ya que sólo nos dice que, si una persona reitera su solicitud en un plazo menor a 12 meses, el responsable puede cobrar hasta tres salarios mínimos. En este supuesto es necesario hacer algunas precisiones como:

a) Se presentan solicitudes sobre diversos derechos.
b) Se presentan solicitudes sobre un mismo derecho, pero diferentes datos.
c) Se presentan solicitudes sobre un mismo derecho y un mismo dato.

Es claro que en el primer supuesto el cobro al que se refiere la Ley no deberá hacerse, pues estamos hablando de un titular que posiblemente primero quiere saber qué datos tiene el responsable de él, luego quiere rectificarlos y posiblemente, en un tercer momento, pretenda oponerse o cancelarlos. En ese sentido se entiende la gratuidad en el ejercicio de los tres derechos.

En el segundo supuesto hablamos de que un titular pudiera ejercer el mismo derecho, pero sobre datos distintos. Este es el caso típico de rectificación, donde en un plazo menor a 12 meses, el titular del derecho solicita la rectificación de dos o tres datos que tiene el responsable. En ese caso, aunque tenemos tres solicitudes del mismo derecho ARCO, debemos entender que en los dos o tres casos se seguirá el principio de gratuidad aún y cuando haya sido ejercido el mismo derecho.

Sólo será en el último de los supuestos planteados donde el responsable podrá hacer efectivo el cobro referido en la Ley y donde el principio de gratuidad presenta una excepción.

Conclusiones

Como hemos podido observar a lo largo del presente comentario, al capítulo IV de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares referente al ejercicio de los derechos de acceso, rectificación, cancelación y oposición, su centro neurálgico se encuentra situado en las medidas de seguridad administrativas que el responsable imponga para un adecuado tratamiento de los datos personales.

Este tratamiento adecuado deberá orientarse por políticas de privacidad y, desde luego, por procedimientos, pues como hemos destacado a lo largo del presente comentario de nada sirve tener un aviso de privacidad si en el seno de la organización no existen las formas en las cuales el titular del derecho puede hacer efectivos sus derechos ARCO.

De igual manera es imperante concluir que los temas contemplados en el comentario pueden adquirir diversos matices, efectos o consecuencias dependiendo el tipo de derecho del cual estemos hablando, pues en la aplicación de la Ley a distintas problemáticas que se presentan en la vida de operación diaria de los responsables, se observa cómo cada ejercicio de derecho requiere un tratamiento diverso respecto a los temas que hemos tratado.

Referencias

Davara, I. (2010*).* "Protección de datos de carácter personal en México: Problemática jurídica y estatus normativo actual*"*, en *Protección de datos personales*. México. H. Cámara de diputados-IFAI-ITAM.

Lucas. P. (2008). "El derecho a la autodeterminación informativa y la protección de datos personales*". Cuadernos de derecho.* Azpilcueta. España. No. 20.

Morte. R. (2017). "¿Protección de datos/privacidad en la época del Big Data, IoT, wearables…? Sí, más que nunca". *Dilemata,* revista internacional de ética aplicada. No. 24.

Solis, C. (2018). "Las medidas de seguridad en materia de protección de datos*"*, en Tenorio, G. (Coord.). *La protección de datos en México. Revisión crítica de su garantía en el ordenamiento jurídico mexicano*. México. TFJA. (en imprenta)

Remolina, N. (2013). "Los derechos de acceso, rectificación, cancelación y oposición en la Ley de datos personales y su reglamento", en Piñar, J. y Ornelas, L. (coords.). *La protección de datos personales en México*. México. Tirant lo Blanch.

Rivero, M. (2018). *El principio de información en materia de protección de datos personales en México*. En Tenorio. México. TFJA. (en imprenta).

Fuentes legales

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Código Civil Federal de México.
Convenio 108 del Consejo de Europa adoptado el 12 de junio del año 2018.

CAPÍTULO V
TRANSFERENCIAS NACIONALES E INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL

CAPÍTULO V
TRANSFERENCIAS NACIONALES E INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL

Artículo 36. *Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.*

El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

Artículo 37. *Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:*

I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;
II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un

tercero;

V. *Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;*

VI. *Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y*

VII. *Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.*

COMENTARIO

Wilma Arellano Toledo[91]

Introducción

Los principios en materia de protección de datos de carácter personal y los derechos asociados a ellos —como son los derechos ARCO que se estudian con detalle en esta obra— encuentran múltiples dificultades en su aplicación y observancia cuando se trata de ciertos procesos que, forzosamente, tienen que llevarse a efecto, como es el caso de las transferencias de datos personales. Máxime si en dicha transferencia la tecnología utilizada es cada vez más avanzada, lo que, por otra parte, sucede muy a menudo en la época actual.

Además, los modelos de protección para las transferencias de datos personales pueden ser muy dispares, dependiendo de la región de que se trate. En México, la Ley adopta un modelo propio, pero el articulado de la misma y su Reglamento también pueden ser analizados a la luz de dos de los principales enfoques en materia de privacidad en el mundo: el europeo y el estadounidense, sin olvidar que es esencial que se garanticen los derechos personales, pero también que no se obstruya el desarrollo comercial y global. En este sentido: "Una de las críticas clave del régimen internacional (de transferencias de datos personales) es el fracaso en cuanto a la satisfacción de las necesidades del entorno empresarial global actual".[92]

De ese modo, los antiguos principios técnicos, reglamentarios y lógicos, y las anteriores medidas de protección de los datos de carácter personal empiezan a convertirse en una base útil, pero sólo eso, una base con una

[91] Capítulo realizado en el marco del proyecto internacional financiado con fondos del Ministerio de Economía y Competitividad de España, denominado: "El avance del Gobierno Abierto. Régimen jurídico constitucional de la implantación de la transparencia, datos abiertos y participación especialmente a través de TIC y E-Gov".

[92] Zwolinska, M. (2015). "International transfers of personal data. Towards a global consensus on data protection standards". *Derecom*. Núm. 19, pp. 165-181.

eficacia limitada frente a cada nuevo desarrollo o evolución de las tecnologías de la información y la Comunicación (TIC). Esta situación ha supuesto la adecuación y actualización de las medidas para la protección de la información referente a las personas físicas identificadas o identificables y, en cuanto se trata de transferencias de datos —e incluso de remisiones de datos— con especial énfasis, como veremos a lo largo de este capítulo.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante LFPDPPP) de 2010[93] tiene un cierto camino recorrido y unos logros asociados a ello, pero aún hay retos importantes que enfrentar. Es un momento ideal de formular un análisis sobre su observancia en cuanto a transferencias de datos personales y exponer posibles mejoras a su contenido.

En este trabajo nos enfocaremos en el capítulo V de la Ley, que se titula "De la transferencia de datos" y que comprende los artículos 36 y 37, referentes a las transferencias tanto nacionales como internacionales de datos. Se considera también el artículo 3, apartado XIX, sobre definiciones. Asimismo, se hace referencia al Reglamento de la LFPDPPP[94] en sus artículos 37, 38 y 39 sobre conservación de datos y al capítulo IV: "De las transferencias de datos personales", así como a los Lineamientos de Protección de Datos Personales.[95] Todo ello, claro está, sin olvidar las correlaciones necesarias con el resto del articulado de estos ordenamientos. De igual forma, se mencionan algunos criterios de los tribunales, sobre este particular y se mencionan ciertos elementos comparativos con el Reglamento General de Protección de Datos de la Unión Europea (RGPD),[96] mismo que entró en vigor en mayo de 2018 y a la fecha de elaboración de este capítulo (octubre de 2018) la UE se disponía "aplicar la primera ronda de multas"[97] derivadas de la omisión de observancia de sus principios y disposiciones.

Las transferencias internacionales de datos podrían requerir medidas adicionales de protección a la información personal, por lo que se mencionarán brevemente algunas normas como las referidas al denominado Puerto Seguro (*Safe Harbour*) y el Escudo de Privacidad (*Privacy Shield*),[98] entre otros.

---

93 Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010 (sin reforma).

94 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el *Diario Oficial de la Federación* el 21 de diciembre de 2011 (sin reforma).

96 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (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); publicado en el *Diario Oficial de la Unión Europea* de 4 de mayo de 2016.

97 Juárez, L. (2018). Europa está lista para aplicar la primera ronda de multas del GDPR. Mediatelecom Tecnología.

98 Recientemente, en la Unión Europea se publicó una resolución al respecto, refiriéndose a los datos personales que se transfieren entre este territorio y los Estados Unidos de América. Se trata de la Resolución del Parlamento Europeo de 5 de julio de 2018, sobre la adecuación de la protección conferida por el Escudo de Privacidad UE-EE.UU.

Correlaciones

Del artículo 67 al 76 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Análisis de contenido

En cuanto a las transferencias de datos, podemos decir, en primera instancia, que hay una diferencia entre dicho concepto y el de las remisiones de datos personales, lo cual conviene aclarar desde un primer momento.

El artículo 3 de la LFPDPPP, de las definiciones, establece claramente que una transmisión es "toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento". El concepto de remisión no aparece claramente señalado en la Ley, pero sí en el artículo 53 de su reglamento, cuando se expone que "las remisiones nacionales e internacionales de datos personales entre un responsable y un encargado no requerirán ser informadas al titular ni contar con su consentimiento".[99]

En cuanto a las remisiones, los Lineamientos del Aviso de Privacidad[100] en el apartado 26, último párrafo, especifican que "el responsable no estará obligado a informar en el aviso de privacidad sobre las comunicaciones de datos personales que existan entre éste y los encargados, lo que se reconoce como remisión [...]".

Con todo esto, queda claro que una transferencia de datos sólo tiene lugar si se da entre un encargado o responsable y un tercero. Cuando los datos circulen entre encargado y responsable, sólo estamos hablando de una remisión de datos de carácter personal.

Por su parte, los lineamientos en materia de protección de datos del INAI (antes IFAI[101]) se refieren a las transferencias de datos personales, a través de las disposiciones concernientes al aviso de privacidad, ya que en este documento se deberá informar debidamente al titular —entre otras muchas objetivos del tratamiento de datos— sobre si sus datos serán objeto de futuras

[99] Antes de ello, el artículo 2 del Reglamento LFPDPPP, en el apartado IX define la remisión como: "La comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano".

[100] Lineamientos del aviso de privacidad de la Secretaría de Economía, publicados en el *Diario Oficial de la Federación* el 17 de enero de 2013.

[101] El órgano garante de los derechos a la transparencia y al acceso a la información y a la protección de datos en México es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), mismo que fuera Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) hasta 2015. Fue en 2005, en pleno periodo de funciones del IFAI, cuando se emitieron los Lineamientos.

transferencias, la finalidad de las mismas y si se trata de transferencias nacionales o internacionales.

En este sentido, puede hacerse una crítica a la diferencia de conceptos o la inclusión y omisión de conceptos entre la LFPDPPP y su reglamento.

Quizá por esta situación y sus consecuencias, el Instituto Nacional de Acceso a la Información y Protección de Datos ha tratado de aclarar las diferencias entre transferencias y remisiones, conceptualizándolas. En la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares [102] se realiza una distinción clara entre ambos conceptos y dedica, además, dos apartados para ilustrar a las empresas sobre las obligaciones que deben cumplir en una remisión entre responsable y encargado y una transferencia entre encargado y tercero.

Entre las obligaciones a cumplir entre responsable y encargado está la de firmar un instrumento jurídico que establezca las condiciones de su relación y los deberes de ambos. Uno de esos deberes es el que tiene el encargado, quien por cuenta propia no podrá transferir datos de carácter personal a un tercero, es decir, sólo puede ejecutar una transferencia cuando sea por orden del responsable, con estricto apego a la norma aplicable y con las adecuadas medidas de seguridad. Más concretamente, el encargado deberá "abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente". Es decir que cuando lo ordena una autoridad, se establece una excepción para que se realice una transferencia sin que el responsable lo haya especificado al encargado.

En la misma guía se especifica que la contravención a esta obligación del encargado (o cuando el responsable realice una transferencia sin el consentimiento del titular) puede implicar multas de 200 a 320 mil días de salario mínimo vigente en la Ciudad de México.

a) Transferencias nacionales de datos en la LFPDPPP y su reglamento

Legislación en la materia

Las transferencias nacionales de datos tienen ciertas características que las diferencian de las internacionales, primero que nada, por la jurisdicción competente en materia de protección de datos de carácter personal y de cualquier asunto que se vincule con la transferencia al realizarse dentro del territorio nacional.

[102] *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (junio de 2016).

Definitivamente, el hecho de que a estas transferencias se les puedan aplicar, uniformemente, los mismos principios (por ser de aplicación directa la LFPDPPP y su reglamento) disminuye la complejidad de las transferencias internacionales de datos.

No obstante, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en sus artículos 36 y 37 no hace especiales diferencias con respecto a una serie de reglas que las empresas y entes privados deben cumplir. De este modo, en el primero de estos dos literales, se expone que: "Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento".

Como se ha explicado a lo largo de este libro en otros capítulos, el consentimiento es el principio sobre el cual descansa el tratamiento legítimo de los datos personales y los titulares deben tener a su disposición la información (otro de los principios) relativa a cómo y para qué se tratará su información personal. Esto sólo sucede por medio de un aviso de privacidad claro y sencillo.[103]

En resumen, la organización, empresa o particular que trate datos personales debe entender que la información personal es un insumo, un activo, pero que no la posee como pasa con otros bienes de la empresa, ya que el titular de los datos es otro y sólo consiente su tratamiento, no se desprende de su titularidad ya que el derecho a la protección de datos es un derecho fundamental, por tanto, imprescriptible e intransferible.

Lo dispuesto en el artículo 36 se resume en que en el momento en que un responsable que maneje datos de carácter personal quiera transferirlos a un tercero que no sea el encargado, deberá darle a conocer el aviso de privacidad que haya puesto a disposición de sus clientes o los titulares de los datos personales. Además, deberá informarle de las finalidades para las cuales se recopilaron los datos.

Si hablamos de garantizar el derecho fundamental a la protección de datos de carácter personal, lo que esta disposición implica es aquello que remarca el artículo 68 del Reglamento de la LFPDPPP y es que "toda transferencia de datos personales, nacional o internacional, se encuentra sujeta al consentimiento de su titular y le deberá ser informada mediante al aviso de privacidad, salvo las excepciones previstas en la Ley".

[103] En este sentido, el artículo 24 del Reglamento establece que: "El aviso de privacidad deberá caracterizarse por ser sencillo, con información necesaria, escrito en lenguaje claro y comprensible, y con una estructura y diseño que facilite su lectura".

Esto es, el responsable que trate datos de carácter personal, en el fondo está cumpliendo con garantizar al titular de los datos su derecho a la autodeterminación informativa, como lo ha llamado la doctrina.[104] Es decir, que las personas conozcan el paradero de sus datos no sólo estando en posesión del responsable que se los ha recopilado, sino también en aquel momento en que los transfiera a un tercero, se encuentre o no en territorio nacional.

Se estarían haciendo efectivos así, por lo menos, cinco de los principios rectores esenciales en la materia que nos ocupa, los cuales son: el de información,[105] el de consentimiento,[106] el de la licitud,[107] el de la finalidad[108] y el de la responsabilidad.[109]

Sin embargo y aunque "por mediar cualquiera de ellos, sea lícito recogerlos [los datos personales] y utilizarlos no significa que el afectado pierda su capacidad de autodeterminación en este ámbito. Al contrario, dispone de una serie de facultades —de derechos— que completan su poder de disposición y de control, empezando por el de revocar la autorización cuando la hubiere

[104] Desde los noventa, catedráticos como Pablo Lucas Murillo De la Cueva, autoridad en la materia, exponían los elementos que giran en torno al concepto de autodeterminación informativa del siguiente modo: "La previsión constitucional de la tutela de los derechos frente al uso de la informática se proyecta sobre los datos personales e implica, por un lado, derechos y garantías para los titulares de esos datos de carácter personal. Por el otro, supone para quienes los recogen, tratan, transmiten, ceden o conservan, una serie de obligaciones en lo que se refiere a la calidad y a la seguridad de la información de esa naturaleza que manejan y a las condiciones en que pueden utilizarla, almacenarla, facilitarla o cederla. Además, implica restricciones a la posibilidad de acceder a ella por parte de terceros, así como límites respecto de los datos personales que pueden ser tenidos en consideración y, posteriormente, incorporados a los ficheros automatizados".
Murillo. L. (1999, abril-junio) "La construcción del derecho a la autodeterminación informativa", en *Revista de Estudios Políticos,* núm. 104, p. 36. En esas restricciones al acceso por terceros es en las que se basan los artículos que regulan las transferencias de datos personales.

[105] El principio de información consiste en dar a conocer al titular de los datos lo referente a cómo serán tratados, con qué fines, si serán transferidos y cómo pueden ejercer sus derechos ARCO, entre otros elementos. Esto implicaría que el consentimiento es informado, como lo disponen la Ley y su reglamento y será un requisito esencial para las transferencias de datos nacionales o internacionales.

[106] Como ya hemos dicho, el consentimiento es el principio sobre el cual descansa el tratamiento lícito y legítimo de los datos personales. Debe ser un consentimiento informado, pero también libre y específico. En materia de transferencias de datos nacionales o internacionales, el consentimiento deberá o debería condicionar que se lleven a cabo o no.

[107] Un tratamiento y, por lo tanto, una transferencia de datos personales entre un responsable y encargado a un tercero, sólo será lícita si media el consentimiento del titular de los datos. El principio de licitud "obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional". Esto es, se debe cumplir con la LFPDPPP y su reglamento, pero también con las normas de derecho internacional y con las disposiciones del país al cual sean transferidos los datos, en caso de tratarse de una transferencia internacional.

[108] La finalidad para la cual fueron recopilados los datos personales debe cumplirse, tal y como se expuso en el aviso de privacidad, cuando los datos estén en posesión del responsable, pero de igual e idéntica manera, cuando estén en posesión de un tercero.

[109] El principio de responsabilidad recae, como aclara con nitidez la Ley y su reglamento, tanto el responsable y el encargado, como en el tercero al que sean transferidos los datos de carácter personal.

prestado".[110] En esencia, como dijimos antes, el titular sigue siendo siempre el dueño de sus datos y puede ejercer su autodeterminación. Incluso revocando su consentimiento. Esta situación, no obstante, puede implicar serios problemas en cuanto a las transferencias de datos personales y en especial, las internacionales como veremos más adelante.

Ahora bien, en la práctica, esta disposición puede ser de sencillo cumplimiento en aquellas empresas que tengan un auténtico control de sus transferencias de datos y un manejo y conocimiento claros de su aviso de privacidad. Pero, además, será posible un completo apego a la Ley cuando los particulares estén en posibilidad de dar a conocer con claridad, a los titulares, aquellos supuestos o situaciones en los que sus datos serán transferidos a un tercero.

De lo contrario, se estaría cumpliendo con la comunicación del aviso de privacidad a un tercero, pero no con el consentimiento del titular de los datos, con lo que se caería en incumplimiento del objetivo marcado en el mencionado artículo 68 del Reglamento. También, si el tercero no adopta las mismas medidas de seguridad o no cumple con los principios rectores o el deber de confidencialidad al recibir los datos transferidos, el responsable caería en incumplimiento, incluso contando con el consentimiento del titular y hasta pudiendo probarlo.

Esto nos enlaza con la segunda parte del artículo 36 de la Ley que estamos comentando, pues se expone que:

> El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

Lo anterior implica, no solamente el citado consentimiento de los clientes, usuarios y titulares de los datos y la obligación de dar a conocer a un tercero (al que se transfieren) el aviso de privacidad, sino que es algo mucho más complejo, y es que dicho encargado se obliga a cumplir con todo lo dispuesto en el aviso que el titular había consentido.

El Reglamento de la LFPDPPP, en concordancia con la Ley, estipula que el responsable deberá obtener el consentimiento del titular, a menos que no sea exigible con arreglo en lo previsto en el artículo 10[111] de la Ley. Esto quiere decir que el consentimiento es necesario en todo caso, a menos que sin él, el

[110] Murillo, L, (2007). "Perspectivas del derecho a la autodeterminación informativa", en *Revista de Internet, Derecho y Política*. Núm. 5, p. 20.

[111] Ese artículo se refiere al principio de licitud del que hemos hablado anteriormente.

tratamiento de los datos personales se siga llevando con apego y cumplimiento a lo dispuesto por la legislación. En el borrador del Reglamento se mencionaba que el consentimiento se tendría que obtener "previo" al tratamiento de los datos. Esa palabra se eliminó en la versión definitiva, posiblemente porque las empresas eran las que tenían la gran mayoría de las bases de datos, y principalmente porque el marco normativo era muy reciente (2011).

Sin embargo, la situación no ha cambiado radicalmente, pues el incumplimiento de las empresas en varios de los preceptos y de los principios rectores tanto de la Ley como del Reglamento, aún es notorio.

Por otro lado, en el artículo 37 —el segundo y último del capítulo V que nos ocupa sobre las transferencias de datos de carácter personal— hay siete apartados sobre el particular, que definen las características que deben tener las transferencias para que estén apegadas a lo dispuesto en la Ley sin necesidad de que el titular de los datos personales otorgue su consentimiento.

Decíamos antes que hay posibilidades de que se realicen transferencias sin el consentimiento del titular, conforme al artículo 10 de la Ley y la licitud del tratamiento.[112] Las transferencias nacionales o internacionales de datos, en este supuesto, podrían realizarse, sin embargo, si cumplen con alguna de las posibilidades descritas en el artículo 37 de la LFPDPPP.

La primera de ellas es que la transferencia de datos de carácter personal se realice sin consentimiento cuando la misma "esté prevista en una ley o tratado en los que México sea parte". Esto, aunque a primera vista permite suponer algo lógico y sin discusión, abre de manera sorprendente un abanico de posibilidades, pues cuando se habla de tratados (esos instrumentos jurídicos internacionales que México ha firmado) las materias sobre las que versan son sumamente diversas. En este punto, consideramos necesario que impere una interpretación y ponderación basadas en la defensa axiomática de los derechos fundamentales reconocidos en nuestra Constitución y en los convenios y declaraciones de derechos humanos (entre los cuales se encuentran el de la protección de datos personales y el de la intimidad y privacidad) por sobre los relativos a materias como el comercio internacional,

[112] La LFPDPPP prevé que el consentimiento no sea necesario para el tratamiento de datos personales siempre y 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; 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, prevención, diagnóstico, 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, o VII. Se dicte una resolución de la autoridad competente".

las negociaciones de defensa y seguridad o los intereses económicos, por mucho que estos aparezcan negociados en un tratado. Por supuesto, este punto en concreto tiene mayor relación con las transferencias internacionales que con las nacionales, aunque también estén implicadas éstas.

El segundo supuesto en el que no se requerirá el consentimiento del titular para realizar una transferencia de datos personales es cuando "sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios". En este caso en concreto, la mayoría de los fines para los cuales se tratan los datos personales podrían parecer incuestionables y altruistas. No obstante, no se debe olvidar que, en este caso en específico, se verían involucrados muchos datos sensibles o especialmente protegidos,[113] por lo que las medidas de seguridad, el deber de confidencialidad y el respeto estricto a los principios rectores de protección de datos personales son sumamente importantes. En cuestión de transferencias de datos de carácter personal, aún más.

El tercer supuesto que puede dar lugar al hecho de que se realice una transferencia de datos personales entre un responsable y un encargado, con un tercero, sin requerir el consentimiento del titular es cuando "la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas".

En realidad, en este punto, si nos atenemos a la interpretación en sentido estricto de las definiciones de la LFPDPPP, es correcto considerar esta excepción, pero si atendemos a la diferenciación que hace el Reglamento, más bien estamos hablando de una remisión de datos de carácter personal y no de una transferencia (incluso siendo internacional). Este es justamente el problema de que en la Ley no se mencionen las remisiones y en el Reglamento sí. En todo caso, si una empresa se apegara a esta excepción para realizar una transferencia sin consentimiento del interesado debe tomar una serie de medidas de seguridad, pero también debe adoptar esa decisión basada en la ética, lo que es primordial para no esconder una transferencia a un tercero con forma de remisión a un encargado o a algunas empresas del mismo grupo.

[113] De acuerdo con el artículo 2, fracción VII de la LFPDPPP y con el artículo 56 de su reglamento, los datos personales sensibles son "aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual". Estos datos sólo pueden formar parte de una base de datos cuando "I. Obedezca a un mandato legal; II. Se justifique en términos del artículo 4 de la Ley, o III. El responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga".

El cuarto supuesto en que una transferencia nacional o internacional de datos personales puede realizarse sin consentimiento del titular es cuando sea "necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero". Esto se ha aplicado, por ejemplo, cuando las empresas alegan fines de facturación o prestación de servicios añadidos, por lo que se consideraría que una transferencia es lícita sin el consentimiento porque no daña los derechos del titular y además le ofrece un servicio adicional o apegado a la contratación entre las partes. Desde luego que esto puede dar lugar a tratamientos no necesariamente auténticos en vista de las características que debería tener la transferencia para llevarse a efecto sin que el titular consienta, por lo que la vigilancia, el ejercicio de los derechos garantizados en la Ley y su reglamento y la autorregulación[114] juegan un papel indiscutiblemente central.

La quinta posibilidad de hacer una transferencia de datos personales lícita sin tener de por medio el consentimiento del titular es cuando sea "necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia". Desde luego, este punto, al igual que varios de los mencionados anteriormente, en primera instancia es totalmente legítimo. Sin embargo, es indispensable del mismo modo que lo son los esquemas éticos y la defensa sin dobleces del derecho fundamental a la protección de los datos de carácter personal, sus principios rectores y los derechos ARCO asociados.

También podrán hacerse transferencias de datos personales sin el consentimiento del titular si se cumple el sexto supuesto que enumera la Ley, que es cuando "sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial".

Finalmente, el último caso en que pueden llevarse a cabo transferencias nacionales o internacionales de datos de carácter personal sin mediar el consentimiento de las personas a las que pertenece la información allí contenida, es cuando "la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular". Esta

[114] Tanto la Ley Federal de Protección de Datos Personales en Posesión de los Particulares como su reglamento incentivan que las empresas adopten códigos éticos y otras medidas de autorregulación en todo lo referente a la protección de los datos y a su tratamiento (artículo 44 LFPDPPP y capítulo VI del RLFPDPPP): "Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la presente Ley... Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos". Pero, además, esos esquemas de autorregulación, que en el Reglamento se adjetivan como vinculantes y que persiguen una armonización con las disposiciones de derecho positivo en la materia, pueden suponer una ventaja para aquella empresa que los ponga en práctica, pues "dicha circunstancia será tomada en consideración para determinar la atenuación de la sanción que corresponda, en caso de verificarse algún incumplimiento a lo dispuesto por la Ley".

posibilidad se amalgama con aquella que describimos anteriormente sobre el cumplimiento de las finalidades definidas en una contratación celebrada entre las partes, por lo que en principio quizá podría integrarse claramente en dicho apartado. Sea del modo que fuere, los comentarios a la aplicación de este supuesto, son los mismos que los señalados para los incisos anteriores.

Ahora bien, antes de pasar a estudiar brevemente alguna sentencia sobre el tema que estamos tratando, es conveniente explicar algunos otros puntos que trata el Reglamento y que tienen relación directa con las transferencias de datos personales. El primero de ellos, que también menciona la Ley, es el que tiene que ver con los plazos de conservación de los datos, puesto que en el artículo 37 del Reglamento se explica que no deben exceder aquellos necesarios para el cumplimiento de las finalidades para las cuales se tratarían lícitamente los datos[115] de acuerdo con lo establecido en el aviso de privacidad.

Desde luego que esto implica una doble problemática puesto que no sólo se trata de que el responsable y su encargado eliminen los datos cuando la finalidad de su tratamiento haya sido cumplida, sino que los eliminen los terceros a los cuales hayan sido transferidos, lo cual supondría un control por parte de la empresa que los recopiló originariamente, puesto que, como claramente dispone el artículo 39 del Reglamento, es en el responsable —como es natural— en quien cae la carga de la prueba, por lo que será él mismo quien deberá asegurarse que así se realice al interior de su organización, pero también con respecto a aquellos datos que haya transferido.

Esto, en la práctica, no es tan sencillo como pudiera pensarse y mucho menos si tomamos en consideración la lógica comercial internacional, la globalización y, sobre todo, las tecnologías de la información y la comunicación (TIC) para las transferencias internacionales y nacionales.

No son pocos los señalamientos que constantemente han realizado las autoridades de protección de datos y privacidad en las reuniones anuales que tienen lugar en distintos lugares del mundo. Una de las alternativas al borrado o eliminación total de los datos personales, cuando la finalidad de su tratamiento haya concluido, es la anonimización. Sin embargo, muchas veces, como ha señalado el Grupo de Trabajo del Artículo 29 de la Unión Europea, el Supervisor Europeo de Protección de Datos y el Parlamento Europeo, se confunden numerosas técnicas de seudoanonimización con hacer los datos realmente anónimos.

[115] Desde luego, no se trataría de una eliminación sin más, sino que se deben "tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos en su posesión previo bloqueo de los mismos, para su posterior supresión".

Como estas autoridades reconocen, muchas veces los datos que supuestamente fueron anonimizados pueden ser nuevamente identificados, con lo cual se les volvería a aplicar la normativa de protección de datos personales. El Reglamento General de Protección de Datos de la Unión Europea, que se publicó en 2016, pero que tiene aplicación directa en todos los países miembros desde mayo de 2018, ha sido muy claro en este sentido, cuando especifica, en su considerando 26, que los principios de protección de datos se aplicarán a la información de personas identificadas o identificables, por lo tanto, los datos seudoanonimizados se consideran aún información personal. Se puede determinar si una persona es todavía identificable a través, por ejemplo, de la singularización "que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física".[116] En el momento en que esto pueda probarse, se trataría de datos anónimos y, por lo tanto, no aplicaría el Reglamento y en el caso mexicano, la LFPDPPP y el Reglamento que utiliza el término de disociación.[117]

Por otro lado, el reglamento de la LFPDPPP dedica el capítulo VI a las transferencias de datos personales. En la sección I del capítulo, el artículo 67 aclara el concepto de transferencia, el 68 establece las condiciones para la transferencia (está sujeta al consentimiento del titular, salvo las excepciones que ya hemos indicado), el 69 se refiere a la carga de la prueba del consentimiento (aquí alude, ya no sólo a la figura del responsable, sino también a la del receptor de los datos, con lo que ello deja abierta la puerta a que dicho receptor sea el encargado, pero también al tercero, o más bien, a este último, ya que estamos hablando de transferencias y no de remisiones) y el 70 que se refiere a las transferencias entre un mismo grupo responsable (en donde se reduce la comprobación de que el receptor cumplirá con las disposiciones de Ley a la existencia de normas internas de protección de datos).

Podría interpretarse que este último artículo se refiere a las excepciones contenidas en el artículo 37 de la LFPDPPP, sin embargo, si nos atenemos a la diferenciación que el propio Reglamento hace entre remisiones y transferencias, tal vez dicha puntualización podría entenderse como presupuesta y por ello no se requiere de consentimiento ni de un compromiso específico de cumplimiento de la finalidad establecida en el aviso de privacidad, sino sólo de la observancia de las normas internas del mismo grupo empresarial.

[116] El Considerando 26 explica que "para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física deben tenerse en cuenta todos los factores objetivos como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos".

[117] De acuerdo con el artículo 3, fracción VIII de 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".

La sección II del capítulo VI del RLFPDPPP se refiere, en sus tres artículos, a las transferencias nacionales de datos personales. El artículo 71 establece las condiciones para dichas transferencias (apegarse a lo dispuesto en los artículos 36 de la Ley y 68 del Reglamento que ya hemos tratado aquí).

El artículo 72 se refiere, específicamente, al receptor de los datos personales y en esta redacción sí que se entiende que se refiere a la figura del tercero al que se realice la transferencia, mismo que debe cumplir con las disposiciones de Ley y con lo contenido en el aviso de privacidad, como responsable en el momento de recibirlas. Incluso, hace notar, levemente, una diferencia entre responsable-receptor y responsable-transferente, aunque sin mencionar explícitamente la primera figura. Esto, nuevamente, podría ser objeto de crítica, dada la disparidad en la redacción del articulado en la Ley y en el Reglamento con respecto a transferencias y remisiones.

Finalmente, el artículo 73 de esta sección (la siguiente la comentaremos en el apartado sobre transferencias internacionales propiamente dichas, porque se refiere específicamente a ellas) trata sobre la formalización de las transferencias nacionales. En este sentido, considera que la "transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable-transferente comunicó al responsable-receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales".

Es decir, que el responsable-transferente comunicó, como lo indica el artículo 36 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, al responsable-receptor las condiciones pactadas en el aviso de privacidad y la finalidad del tratamiento tras el consentimiento del titular de la información personal. Con esto se estaría cumpliendo con una parte de lo que determina la Ley, pero haría falta el control posterior que ya hemos mencionado, de lo que realice el receptor, sobre todo cuando la finalidad del tratamiento se haya cumplido.

b) Jurisprudencia y criterios nacionales en materia de transferencias de datos personales

Aunque ya existe un camino recorrido desde la publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su reglamento un año después, aún es poca la jurisprudencia que podemos encontar en cuanto a las transferencias de datos personales se refiere, a diferencia de otros aspectos de la normativa. Quizá en buena medida porque algunos de los criterios para la aplicación de la Ley o para la puesta efectiva en marcha de una transferencia se deriven también de otros ordenamientos o instrumentos que van más allá del ámbito nacional.

Debido a la escasez de criterios en materia de transferencias de datos personales y al espacio con el que contamos en este capítulo (pues su contenido esencial es el análisis de la LFPDPPP) vamos a mencionar sólo una sentencia, que además es muy reciente. Se trata de la Tesis del Pleno del Tribunal de Justicia Fiscal y Administrativa referente a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en el juicio contencioso administrativo número 23263/15-17-14-1/1107/16-PLE-09-04 (18 de abril de 2018).[118] En la sentencia, el TJFyA interpreta que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales no es competente para iniciar el procedimiento de protección de datos con respecto a una empresa situada fuera del territorio nacional. La interpretación se hace a la luz de lo dispuesto en el artículo 1 de la Ley[119] y al 4 de su Reglamento.[120]

En concreto, el Tribunal determina que el INAI "no será competente en razón de territorio para iniciar el procedimiento de reconocimiento de protección de datos en contra de una persona extranjera si no se acredita que ésta cuenta con una sucursal u oficina de representación en el territorio mexicano".

Si bien, en primera instancia este criterio hace pensar en cierta indefensión de una persona cuando solicita protección a un órgano constitucional autónomo como es el INAI frente a un tratamiento de datos personales que bien puede ser consecuencia de una transferencia entre un responsable y un tercero, no debemos olvidar que existen otras vías a nivel supranacional para amparar los derechos reconocidos y garantizados en la Declaración Universal, los convenios, los pactos y en la Constitución de nuestro país.

Así, en concordancia con la vía jurisdiccional de protección de los derechos humanos, el artículo 28 de la Declaración Universal de los Derechos Humanos que se refiere al ámbito internacional y que sentará las bases para que se conformen las autoridades a ese nivel: "Toda persona tiene derecho a que se establezca un orden social e internacional en el que los derechos y libertades proclamados en esta Declaración se hagan plenamente efectivos".[121]

---

[118] Tesis no. 8-P-SS-247, *Revista del Tribunal Federal de Justicia Administrativa,* número 26, septiembre de 2018, pp. 44-45

[119] En cuanto al ámbito de aplicación de la Ley que sostiene que "la presente Ley es de orden público y de observancia general en toda la República".

[120] Sobre el ámbito territorial de aplicación de la Ley que reza que el reglamento "será de aplicación obligatoria a todo tratamiento cuando I. Sea efectuado en un establecimiento 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, y IV. El responsable no esté establecido en territorio mexicano y utilice medios situados en dicho territorio".

[121] Sobre la eficacia de los derechos humanos, también Silva y Silva sostienen que tales derechos, como parte integrante de la Carta Magna, "son predicables directamente frente a los poderes públicos (eficacia vertical) y frente a los particulares (eficacia horizontal)". Es por ello que, con

Se observa con claridad la referencia a ese sistema universal aunque no se mencionan las autoridades competentes para tal efecto.[122]

Si "el sistema universal está en completa consonancia con los sistemas nacionales y regionales",[123] la protección de un derecho como el de la protección de los datos de carácter personal, puede ser plenamente efectiva, aunque, con sentencias como la mencionada —aun entendiendo la interpretación que hace el Tribunal de Justicia Fiscal y Administrativa— pueden hacer el camino más complejo para una persona que quiera defender su derecho fundamental.

También algunos otros tribunales han dictado sentencias que guardan relación con las transferencias de datos de carácter personal.[124]

c) Transferencias internacionales de datos: marco legal nacional y otros marcos internacionales

Aunque todas las transferencias de datos de carácter personal deben seguir principios e integrar una serie de medidas de seguridad son, sin duda, las transferencias internacionales las que más complejidad representan puesto que intervienen las legislaciones, jurisdicciones y exigencias de cada uno de los países involucrados. Como ya vimos en el apartado anterior, todas las disposiciones de los artículos 36 y 37 de la LFPDPPP son de aplicación tanto a las transferencias nacionales como las internacionales, por lo que ahora sólo nos vamos a referir a los preceptos específicos del Reglamento para las transferencias internacionales o transfronterizas.

---

respecto a la eficacia vertical, los poderes públicos deben hacer efectivos los derechos humanos a través de la acción legislativa y jurisdiccional, lo cual va encaminado en la línea de lo que estamos tratando. Silva, J. y Silva, F. (2013) *Derechos fundamentales. Bases para la reconstrucción de la jurisprudencia constitucional*. México. Editorial Porrúa. pp. 108.

122 A diferencia del ámbito global en la DUDH, en el regional sí se estipula qué autoridades serán competentes en materia de derechos humanos a través del artículo 33 de la Convención Americana de los Derechos Humanos, el cual establece que "son competentes para conocer de los asuntos relacionados con el cumplimiento de los compromisos contraídos por los Estados partes" tanto la Comisión Interamericana de Derechos Humanos como la Corte Interamericana de Derechos Humanos. Además, en el texto de la Convención se establece la manera en que se conformarán ambas instancias, sus funciones, niveles competenciales y los procedimientos para solicitar su actuación por parte de cualquier persona.

123 Arellano, Wilma. (2013). "Sistema universal de derechos humanos: sistema jurisdiccional y no jurisdiccional", en *Derechos Humanos y Seguridad Pública.* México. Instituto Latinoamericano de Comunicación Educativa.

124 Por ejemplo, el séptimo Tribunal Colegiado en Materia Administrativa del Primer Circuito en su tesis: I.7o.A.635A, referida a la suspensión en el amparo, dice que "debe negarse contra los efectos y consecuencias de los lineamientos por los que se determina la operación y funcionamiento del registro público de usuarios —personas físicas— que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios, ya que su concesión afectaría el interés social y contravendría disposiciones de orden público" (Séptimo Tribunal Colegiado en Materia Administrativa del Primer Circuito. Incidente de suspensión (revisión) 105/2009. Financiera Finsol S.A. de C.V. Sociedad Financiera de Objeto Múltiple. Entidad no Regulada. 22 de abril de 2009. Unanimidad de votos).

Es importante señalar que las transferencias internacionales de datos personales suelen tener lugar en los procesos de comercio fuera del país en el que tiene su residencia el responsable y, puede ser, que también del encargado. Para hacer frente a los desafíos de la globalización, las empresas tienden a internacionalizarse para buscar otros mercados y conseguir más y mejores cifras de negocio, pero cuando se trata de transacciones u operaciones en las que se implique una transferencia de datos de carácter personal a nivel internacional, es sumamente importante cumplir con la normativa aplicable.

En el caso de México, al desarrollar actividad económica con otros países, pero —en cuanto a rigurosidad— especialmente con la Unión Europea (UE) es esencial que se observe no sólo la LFPDPPP y su reglamento, sino una serie de reglas (entre las que pueden estar las corporativas vinculantes y los esquemas de autorregulación) entre empresas y una serie de ordenamientos del país o la región a la que se pretendan transferir los datos, pero más aún, cuando se pretenda recibir datos personales de países de dicha comunidad de Estados. Las directivas europeas han sido siempre muy estrictas en cuanto a la observancia de principios y de derechos de los titulares de los datos y el actual Reglamento General de Protección de Datos (que tiene aplicación directa en todos los países miembros) no es menos severo en ese sentido.[125]

La UE ha establecido, a través de dichos instrumentos jurídicos, que los datos de carácter personal de ciudadanos comunitarios sólo pueden formar parte de flujos transfronterizos cuando el país de destino tenga un "nivel adecuado de protección" y sea revisado constantemente.[126] Así, las empresas mexicanas que cumplan con la LFPDPPP y su reglamento, también deben tomar en cuenta las reglas y medidas de seguridad adicionales que pueda solicitar cumplir la Unión Europea, en caso de querer realizar transacciones con los países que la integran.

No obstante, no solamente la UE es una región con la que existen intercambios importantes de información —entre la que se encuentra la de carácter personal. Hay también otras regiones, como Norteamérica (para la cual también rigen otra serie de acuerdos y convenios importantes), Sudamérica

[125] Incluso, hay quien sostiene que "la normativa de la Unión Europea en el campo de la protección de datos es la más exigente del planeta" y puesto que hay países en donde sucede todo lo contrario "se han regulado minuciosamente las transferencias internacionales de datos" Guash, V. (2012). "La transferencia internacional de datos de carácter personal". *Revista de Derecho UNED*. Núm. 11, pp. 413-453.

[126] Al respecto, "para llegar a un pronunciamiento sobre el carácter adecuado (o no) del nivel de protección concedido en terceros Estados [distintos de los Estados miembros de la UE], se ha de valorar periódicamente el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales de éste, así como la práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país". Mendoza, A. (2015). "Transferencias internacionales de datos personales: Estados Unidos no es un puerto seguro, pero tampoco una isla inalcanzable". *Revista de Derecho de Consumo.* Núm. 15, p. 213.

(para la que existen acuerdos con algunos países) o la de Asia-Pacífico (región a la que pertenece México y que se rige por diversos instrumentos y documentos de la APEC).[127]

De hecho, en 2004 la APEC adoptó una serie de parámetros en materia de privacidad y protección de datos para asegurar el libre flujo de datos transfronterizos sin la necesidad de vulnerar la protección de dichos datos. Derivado de estos parámetros surgió la necesidad de establecer un sistema para aterrizarlos y se creó el Sistema de Reglas de Privacidad Transfronteriza.

Ahora bien, antes que todo eso, una empresa o particular mexicano que quiera realizar una transferencia internacional de datos de carácter personal, además de cumplir con lo dispuesto en la LFPDPPP debe observar lo estipulado en la sección III del capítulo VI del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

A la luz de lo dispuesto en la Ley, comentaremos los tres artículos que comprende. El artículo 74 del Reglamento va un poco más allá de lo establecido en el artículo 36 de la Ley (y sin perjuicio de lo que impone el 37) pues ordena que para que una transferencia internacional pueda tener lugar, el responsable receptor debe asumir "las mismas obligaciones que corresponden al responsable que transfirió los datos personales".

En la práctica, esto puede ser un obstáculo para determinadas transferencias internacionales con terceros países, tanto si en el lugar de destino la legislación es más flexible como si es mucho más rígida que la mexicana a través de la LFPDPPP y su reglamento. Si se trata de un país en donde las normas son más flexibles e incluso inexistentes, el grado de cumplimento que exige nuestra Ley Federal puede ser tan elevado e implicar procedimientos tan onerosos o engorrosos —por no estar establecidos de forma natural allí— que puede desincentivar el flujo transfronterizo de información personal y, con ello, ciertas actividades comerciales y económicas, e incluso, de cooperación internacional. Si el grado de exigencia en el país de destino es más rígido que el mexicano, aquel receptor puede exigir, a su vez, que el responsable sujeto a la LFPDPPP adopte las medidas establecidas en su territorio para conseguir la igualdad de intereses en los acuerdos que impliquen la transferencia de datos de carácter personal. Estos procesos ocurren frecuentemente en la realidad actual, tanto en un sentido como en otro y son los responsables los que tienen que tomar decisiones al respecto y no olvidar la función de los

[127] Foro de Cooperación Económica Asia-Pacífico (*Asia-Pacific Economic Cooperation*) conformado por 21 países entre los que se encuentran México, Estados Unidos, Canadá, gran parte de Asia, algunos países de América Latina y Australia, entre otros. Su marco general sobre privacidad está enfocado a que la protección a la misma, no empañe las relaciones comerciales y el crecimiento económico regional.

esquemas de autorregulación y las normas corporativas vinculantes (de las que hablaremos en breve).

El ejemplo clásico de la disparidad de criterios en cuanto a la protección de datos personales es el que afecta a los flujos transfronterizos o transferencias internacionales entre Estados Unidos y la Unión Europea. El país norteamericano exige cada vez más información personal, no sólo en transacciones comerciales, sino en cuanto a los viajeros que lo visitan. En cambio, la UE exige cada vez mayor protección de los datos de carácter personal de los ciudadanos de la Comunidad Europea, y en la actualidad, con mayor razón, tras la entrada en vigor del Reglamento General de Protección de Datos.

En este sentido, desde hace décadas, ambas regiones han establecido una serie de criterios —a través de diversos acuerdos— para regular las transferencias internacionales entre ellos. Uno fue el denominado Acuerdo del Puerto Seguro (*Safe Harbour*) que tuvo validez desde 2000[128] hasta octubre de 2015 y que fue sustituido por el actual Escudo de Privacidad (*Privacy Shield*).[129] Ahora, para determinar que hay un "grado de protección adecuado" y se pueden transferir los datos, tiene que haber un acuerdo de conformidad: "es una decisión adoptada por la Comisión Europea que establece que un país no perteneciente a la Unión garantiza un adecuado nivel de protección de los datos de carácter personal en virtud de su legislación propia y los acuerdos internacionales...Con ésta, los datos personales podrán transferirse desde los 28 Estados miembros (y los tres miembros del Espacio Económico Europeo: Noruega, Liechtenstein e Islandia) a un tercer país".[130]

Volviendo al Reglamento, el artículo 75 de la Sección III en comento, dispone, por su parte, las condiciones para la formalización de las transferencias internacionales. Es decir, aquellas específicas que deben cumplirse como las estipuladas en el artículo 73 del Reglamento sobre formalización de transferencias nacionales. En este caso, el Reglamento añade que el responsable que transfiere podrá hacer uso de "cláusulas contractuales o algunos otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable

[128] Decisión de la Comisión del 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de Puerto Seguro para la protección de la vida privada las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, publicada en el *Diario Oficial de las Comunidades Europeas* el 25 de agosto de 2000.

[129] Resolución del Parlamento Europeo del 5 de julio de 2018 sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-USA, publicada en el *Diario Oficial de la Unión Europea* el 23 de agosto de 2018.

[130] INCIBE (Instituto Nacional de Ciberseguridad). (2016). *Adiós Puerto Seguro, bienvenido Escudo de Privacidad*. Disponible en: *https://www.incibe.es/protege-tu-empresa/blog/adios-puerto-seguro-bienvenido-escudo-privacidad* Fecha de consulta: 10 de octubre 2018.

que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales".

Este deber ya se especificó también en la guía para cumplir con los principios y deberes de la Ley de Protección de Datos que elaboró el INAI (entonces IFAI) y que citamos cuando hablamos de las diferencias entre remisiones y transferencias de datos de carácter personal.

Sin duda, se trata de una obligación (aunque el artículo establece que "podrá valerse", lo que deja a libre albedrío a la empresa para añadirlo al instrumento jurídico señalado en el literal 74) que al mismo tiempo puede ser una garantía sumamente importante para las empresas que hagan transferencias internacionales de datos personales, pues esto las protege de su posible incumplimiento y la consecuente sanción por parte de la autoridad competente, que es el INAI. Sin embargo, plantea la misma dinámica con respecto a lo establecido en el artículo 74 del Reglamento que recién comentamos: la posible disparidad en el rigor de unos ordenamientos y otros.

Para lo que sí es sumamente útil la utilización de las cláusulas contractuales que menciona el artículo 75 del Reglamento es para aquellos casos en los que haya, además de una transferencia internacional, un uso de medios tecnológicos como el denominado cómputo en la nube (*cloud computing*). El mismo Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares contiene un apartado relativo a esta tecnología. En el artículo 52 se refiere al cómputo en la nube y a las medidas que un responsable y un encargado deben tomar cuando realicen subcontratación o externalización de servicios con *cloud*. Naturalmente, esas precauciones son perfectamente válidas para las transferencias de datos de carácter personal, internacionales o no.

En este sentido, cabe mencionar que con el cómputo en la nube y teniendo de por medio las transferencias internacionales, "los datos del cliente pueden estar moviéndose entre distintos países, algunos de ellos con protección adecuada de los datos personales, pero otros que no disponen de esta protección".[131]

Asimismo, el proveedor de servicios en la nube se encarga de garantizar la seguridad física en sus centros de procesos de datos. Por ejemplo, tomando medidas físicas como las que menciona la LFPDPPP y su reglamento para impedir accesos no autorizados y hurtos de equipos o sistemas también deberá mantener sus equipos actualizados, tanto *hardware* como *software*, para hacer frente a las amenazas existentes en internet. Para esto, se utilizan

[131] Guash, V. (2017). "La computación en nube y las transferencias internacionales de datos en el nuevo reglamento de la UE". *Revista de Derecho UNED*. Núm. 20, p. 333.

mecanismos "como la virtualización y la segmentación de datos para reforzar la seguridad de sus servicios en la nube".[132]

Para terminar con el contenido del Reglamento de la Ley de Datos Personales en materia de transferencias internacionales, abordaremos su artículo 76 en donde se insta a los responsables de las transferencias a consultar al INAI y solicitar su "opinión respecto a si las transferencias internacionales que realicen cumplen con lo dispuesto por la Ley y el presente Reglamento".

Por supuesto que lo anterior es válido. Sin embargo, en la realidad es bastante complicado atender una gran cantidad de solicitudes de opinión por parte del INAI, que tendría que hacer una valoración estudiada de los casos, los cuales son complejos y por eso son sometidos a consulta. Del mismo modo, para una empresa puede ser engorroso y lento esperar a que el Instituto responda, pues los tiempos para realizar las transacciones comerciales, económicas y hasta en cuanto a cooperación, pueden requerir una presteza mayor.

Resumiendo, de acuerdo con los elementos mínimos que debe contener el aviso de privacidad y lo dispuesto en la LFPDPPP y su reglamento, las empresas deberán adoptar medidas adicionales dependiendo del tamaño de su organización, de las características físicas o electrónicas de sus bases de datos, de las transferencias que hagan a terceros (los cuales deberán asumir las mismas responsabilidades que el responsable, como hemos insistido a lo largo de este capítulo), de los acuerdos, convenios o normas vinculantes que firmen con otros agentes del mercado, de las medidas de seguridad que tengan, pero también de las que carezcan en el momento de transferir información personal, así como de las normas del sector al que pertenezcan (pueden ser más valiosas, económicamente hablando, las bases de unos sectores a otros y en algunos casos, contendrán datos sensibles).

En cuanto a las medidas de seguridad que adquieren una especial relevancia cuando hablamos de transferencias internacionales de datos de carácter personal, tanto la Ley como su reglamento se refieren a ellas como fundamentales para garantizar que el responsable, el encargado y el tercero cumplan con lo dispuesto en el aviso de privacidad, atiendan a la finalidad del tratamiento, eliminen los datos personales cuando dicha finalidad se haya cumplido y concluyan con el deber de confidencialidad.[133] Las medidas de

[132] Instituto Nacional de Tecnologías de la Comunicación (INTECO). (2011), en *Guía para empresas: seguridad y privacidad del cloud computing*. Madrid, p. 34.

[133] Además del deber de seguridad, los responsables, encargados y terceros deben cumplir con el deber de confidencialidad que implica una "obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable", de acuerdo con el artículo 21 de la LFPDPPP y 9 del Reglamento.

seguridad pueden ser administrativas,[134] técnicas[135] y físicas,[136] según lo dispuesto en el artículo 19 de la LFPDPPP.

Con respecto a las normas vinculantes, éstas son esenciales en el marco de las transferencias internacionales de datos (aunque también son de suma utilidad en las nacionales), puesto que hoy en día se desarrollan en el contexto de la globalización y el desvanecimiento de fronteras en el entorno de las TIC y la sociedad de la información.

Así que es necesario que las compañías adopten reglas como las Normas Corporativas Vinculantes (*Binding Corporate Rules,* BCR) ya que de lo contrario podrían, incluso, aislarse de la competencia en el nivel internacional. Las BCR implican esquemas de autorregulación y permiten armonizarse con las disposiciones legales del derecho positivo. Además, pueden ser un complemento de mucha utilidad cuando los marcos jurídicos son dispares entre los países que lleven a cabo una transferencia internacional que incluya datos de carácter personal.

Un grupo de empresas multinacionales estipulan dichas normas y establecen una serie de principios mínimos con los que serán tratados los datos personales que interfieran en las relaciones mercantiles para proteger la privacidad de los usuarios de los países implicados. Asimismo, las empresas deben respetar las medidas nacionales sobre protección de datos y privacidad, pero también aquellas internacionales que afecten a su labor y/o cooperación con la industria internacional.

La Agencia Española de Protección de Datos (AEPD) las define como "las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo

[134] El artículo 2 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en su apartado V define las medidas de seguridad administrativas como aquellas que implican un "Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación de personal en materia de protección de datos personales".

[135] Las medidas de seguridad técnicas, en el mismo artículo 2 del Reglamento en su apartado VII, se conceptualizan como "conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar" que el acceso a las bases de datos sea por los usuarios autorizados y que actúen cumpliendo con sus funciones; que se lleven a cabo acciones para comprar equipos seguros y que se efectúe "la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales"

[136] Finalmente, las medidas físicas son definidas por el reglamento de la Ley en el mismo artículo 3, pero apartado VI como el "conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados" a impedir accesos no autorizados o daños a las bases de datos, a proteger los equipos y procurar que éstos sean funcionales y a garantizar la eliminación de la información de forma segura.

empresarial o una unión de empresas dedicadas a una actividad económica conjunta".

Aunque la AEPD se refiere claramente a las transferencias entre España o países de la Unión Europea con terceros, la definición es aplicable a todas las transferencias internacionales de datos personales. Además, las considera fundamentales cuando la UE no reconoce un "grado de protección adecuado" en el país de destino.

Conclusiones

Definitivamente, el régimen relativo a las transferencias de datos de carácter personal contenido en el capítulo V de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y que está regulado por su correspondiente reglamento tiene una notable complejidad. En primer lugar, porque las transferencias de datos personales son imprescindibles, no sólo a nivel nacional sino internacional —aunque estas últimas son las más problemáticas por las diferentes jurisdicciones y las competencias que se pueden mezclar en una determinada transferencia.

En segundo lugar, porque las TIC implican una serie de procesos que desafían las lógicas tradicionales en materia de protección de las bases de datos, incluidas aquellas que contienen datos personales. Además, la legislación se ve superada, pues aunque, tanto la LFPDPPP como su reglamento hacen referencia a las medidas de seguridad técnicas que un responsable debe asumir para proteger los datos personales de los titulares y también se menciona el cómputo en la nube, muchos son los desafíos que las empresas tienen que afrontar en la práctica para hacer valer los principios de protección de datos y cumplir con sus deberes de seguridad y confidencialidad, mucho más si se ven involucrados procesos, metodologías computacionales o tendencias tecnológicas como el big data o el internet de las cosas.[137]

No sólo las TIC (que acentúan mucho el problema) sino incluso el cumplimiento de obligaciones tales como el hecho de asegurarse que el tercero que reciba una transferencia de datos de carácter personal cumple con las medidas de seguridad del responsable y el encargado, acata lo establecido en el aviso de privacidad y respeta el principio de finalidad para el cual se deberán tratar los datos personales; todo lo cual es muy complicado en la práctica.

[137] El internet de las cosas, también llamado internet de los objetos, implica la conectividad de diversos dispositivos, aparatos, redes, enseres, ropa, accesorios y hasta alimentos. De este modo, "entrando en diversos terrenos que pueden englobar una serie de datos personales —sensibles o no—, con el consecuente riesgo de violar la privacidad de los individuos o, peor aún, si se trata de los datos especialmente protegidos, dando lugar a discriminación, atentando contra la dignidad de la persona". Arellano. W. (2017, enero- marzo). "Privacidad e Internet de las Cosas (IoT)". *Revista de Privacidad y Derecho Digital*. Vol. 2. Núm. 6, p. 26.

Sin embargo, para complementar las disposiciones de la Ley y su reglamento, ambos incentivan la adopción de esquemas de autorregulación vinculante y se recomienda optar por instrumentos jurídicos específicos para las transferencias de datos de carácter personal, cláusulas precisas y las Normas Corporativas Vinculantes (BCR por sus siglas en inglés), entre otras medidas.

Referencias

Arellano. W. (2017, enero- marzo). "Privacidad e Internet de las Cosas (IoT)". *Revista de Privacidad y Derecho Digital*. Vol. 2. Núm. 6, pp. 25-56.

_____. (2013). *Sistema universal de derechos humanos: sistema jurisdiccional y no jurisdiccional. Derechos Humanos y Seguridad Pública.* México. ILCE.

Guash, V. (2017). "La computación en nube y las transferencias internacionales de datos en el nuevo reglamento de la UE". *Revista de Derecho UNED*. Núm. 20, pp. 333-349.

_____. (2012). "La transferencia internacional de datos de carácter personal". *Revista de Derecho UNED*. Núm. 11, pp. 413-453.

Juárez, L. (2018*). Europa está lista para aplicar la primera ronda de multas del GDPR*. Mediatelecom Tecnología.

Martínez, Ricard. (2016, febrero-mayo). "Privacidad, Estados Unidos y España. Tan lejos, tan cerca". *Telos. Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad.* Núm. 97, pp. 48-56.

Mendoza, A. (2015). "Transferencias internacionales de datos personales: Estados Unidos no es un puerto seguro, pero tampoco una isla inalcanzable". *Revista de Derecho de Consumo*. Núm. 15, pp. 212-227.

Minero, G. (2015). "Avances en la regulación europea del derecho a la protección de datos personales y el derecho al olvido". En Bueno de Mata, F. (coord.). *Fodertics 4.0. Estudios sobre nuevas tecnologías y justicia.* Granada. Comares, pp. 77-91.

Murillo, L. (1999, abril-junio). "La construcción del derecho a la autodeterminación informativa". *Revista de Estudios Políticos.* Núm. 104, pp. 35-60.

_____. (2007). "Perspectivas del derecho a la autodeterminación informativa". *Revista de Internet, Derecho y Política.* Núm. 5, pp. 18-32.

Ortega, A. (2016, febrero-mayo). "Algunas claves en las relaciones entre los EEUU y la UE sobre transferencias de datos de carácter personal. El acuerdo de Puerto Seguro". *Telos. Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad.* Núm. 97, pp. 57-63.

Silva, J. y Silva, F. *Derechos fundamentales. Bases para la reconstrucción de la jurisprudencia constitucional.* México. Editorial Porrúa, p. 540.

Zwolinska, M. (2015). "International transfers of personal data. Towards a global consensus on data protection standards". *Derecom*. Núm. 19, pp. 165-181.

CAPÍTULO VI
DE LAS AUTORIDADES

CAPÍTULO VI
DE LAS AUTORIDADES

SECCIÓN I
DEL INSTITUTO

Artículo 38. *El Instituto, para efectos de esta Ley, tendrá por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento.*

Artículo 39. *El Instituto tiene las siguientes atribuciones:*

I. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación;

II. Interpretar en el ámbito administrativo la presente Ley;

III. Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley;

IV. Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables de esta Ley, para efectos de su funcionamiento y operación;

V. Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable;

VI. Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en esta Ley e imponer las sanciones según corresponda;

VII. Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos;
VIII. Rendir al Congreso de la Unión un informe anual de sus actividades;
IX. Acudir a foros internacionales en el ámbito de la presente Ley;
X. Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes;
XI. Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en Posesión de los Particulares y brindar capacitación a los sujetos obligados, y
XII. Las demás que le confieran esta Ley y demás ordenamientos aplicables.

SECCIÓN II
DE LAS AUTORIDADES REGULADORAS

Artículo 40. *La presente Ley constituirá el marco normativo que las dependencias deberán observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda, con la coadyuvancia del Instituto.*

Artículo 41. *La Secretaría, para efectos de esta Ley, tendrá como función difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano; promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto.*

Artículo 42. *En lo referente a las bases de datos de comercio, la regulación que emita la Secretaría, únicamente será aplicable a aquellas bases de datos automatizadas o que formen parte de un proceso de automatización.*

Artículo 43. *La Secretaría tiene las siguientes atribuciones:*

I. Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial;
II. Fomentar las buenas prácticas comerciales en materia de protección de datos personales;

III. Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad en coadyuvancia con el Instituto, a que se refiere la presente Ley;

IV. Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general a que se refiere el artículo 40, en coadyuvancia con el Instituto;

V. Fijar los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere el artículo 44 de la presente Ley, incluido la promoción de Normas Mexicanas o Normas Oficiales Mexicanas, en coadyuvancia con el Instituto;

VI. Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento;

VII. Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales;

VIII. Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales;

IX. Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial, y

X. Apoyar la realización de eventos, que contribuyan a la difusión de la protección de los datos personales.

Artículo 44. *Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la presente Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento.*

Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares. Dichos esquemas serán notificados de manera simultánea a las autoridades sectoriales correspondientes y al Instituto.

COMENTARIO

Luis Ricardo Sánchez Hernández

Introducción

El lunes 1 de junio de 2009 se publicó en el *Diario Oficial de la Federación* (DOF) el decreto por el que se adicionó un segundo párrafo (recorriéndose los subsecuentes en su orden) al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, con lo que el derecho a la protección de datos personales obtuvo reconocimiento constitucional en nuestro país como un derecho humano.

Si bien es cierto que este derecho ya se encontraba inserto en el artículo 6, a partir de la reforma constitucional publicada en el DOF el 20 de julio de 2007 en lo que hoy conforma el apartado A, su ámbito de protección se circunscribía al sector público como una limitante al ejercicio del derecho de acceso a la información.

En el mismo sentido, mediante un decreto publicado en el DOF, el 30 de abril de 2009, a través del cual se adicionó la fracción XXIX-O al artículo 73 constitucional, se incorporó, como facultad del Congreso de la Unión, legislar en materia de protección de datos personales en posesión de particulares, con lo cual, dicha materia queda comprendida dentro de la competencia federal. Atendiendo la distribución residual prevista por el artículo 124 de la Constitución, se restringe la facultad a las entidades federativas de legislar sobre la materia, delimitando el régimen aplicable, pero sin constituir un derecho fundamental.

Así, de manera aparente, la reforma del 1 de junio de 2009 brindó coherencia normativa respecto a los regímenes aplicables del sector público y el de particulares, no obstante, dadas las características que revisten las condiciones de tratamiento en el ámbito de particulares ¿Es susceptible de tener en cuenta dichos supuestos como derechos fundamentales? Si no es así, ¿cuál fue el sentido de la adición de dicho párrafo si en la práctica resultaba suficiente su inclusión dentro del artículo 6 constitucional?, ¿es dable considerar como derecho fundamental la protección de datos personales en posesión de los particulares al no existir distinción expresa en el texto del segundo párrafo del artículo 16 de nuestra Constitución?

Sobre el particular, es interesante teorizar acerca de las implicaciones de la reforma constitucional en comento en contraste con las teorías contemporáneas en materia de derechos humanos y los nuevos modelos de gobernanza orientados a la transparencia colaborativa y el desarrollo sostenible, en donde las grandes empresas tecnológicas adquieren una dimensión social que rebasa

sus fines meramente económicos y en los cuáles, con el uso de tecnologías y la desaparición de intermediarios, las divisiones entre lo público y lo privado son cada vez más delgadas, y en ocasiones, parecería que tienden a desaparecer.

Ante dichas circunstancias, el imperativo tecnológico ha modificado las exigencias para los gobiernos y las administraciones públicas ante la oferta de bienes y servicios que, tradicionalmente, se encontraban bajo su potestad, pero que ante la demanda ciudadana y la democratización digital han debido allanarse, como en el caso de empresas como Uber, Cabify, Didi, entre otras, que en la práctica prestan servicio público de transporte, pero que en la forma, realizan un servicio privado, dado el mecanismo o tecnología utilizados para tal efecto, y por tanto, no requieren obtener una concesión o permiso por parte del Estado.

Aunado a los diversos servicios que han generado disrupción con los modelos digitales, las tecnológicas de facto constituyen actores de peso dentro de la gobernanza en internet, en demérito de la organización *multistakeholder*, y por ende, cuentan con poderes fácticos y económicos que rebasan las capacidades administrativas, financieras y de inteligencia de varios países y que tienen repercusión en los derechos de las personas, como en el caso de la libertad de expresión, en donde los motores de búsqueda como Google y las redes sociales, como Facebook, Twitter e Instagram modifican, conforme ciertos parámetros, la información disponible para el usuario dependiendo el algoritmo, y por ende, resulta factible determinar la información que se podrá visualizar en la plataforma.

Estos supuestos todavía escapan del ámbito de estudio de los derechos fundamentales pues resultan atribuibles a empresas particulares a pesar que de manera formal ya se reconoce la posibilidad de la afectación por parte de particulares al serles reconocido el carácter de autoridades responsables en un juicio de amparo, tal como lo previene el artículo 5 fracción II, segundo párrafo de la Ley de Amparo de la manera siguiente: "Para los efectos de esta Ley, los particulares tendrán la calidad de autoridad responsable cuando realicen actos equivalentes a los de autoridad, que afecten derechos en los términos de esta fracción, y cuyas funciones estén determinadas por una norma general".

Reflexión a partir de la cual se deja a la opinión del lector la validez o no de las preguntas y respuestas formuladas previamente, ya que como en cualquier otra disciplina sujeta al rigor de la ciencia o el método, los resultados se reflejan en el transcurso del tiempo y estamos en un momento temprano, dentro de la era digital, en el cual es complicado predecir cuáles serán los efectos transformadores de las relaciones humanas a partir de las disrupciones provocadas por las TIC.

Teniendo como eje instrumentador el derecho a la protección de datos personales en torno a la tutela de la privacidad, la intimidad y la autodeterminación informativa, se aprecia que, tratándose de esta última, resulta desproporcionado trasladar hacia el titular de los datos los deberes relativos a su seguridad a través de la autodisposición, ya que como ha podido atisbarse, el papel actual de las tecnológicas rebasa, por mucho, las capacidades de organizaciones y naciones, por lo que surge una segunda vertiente de la autodeterminación: el entorno seguro facilitado por el Estado y asegurado por instituciones dedicadas a dicho fenómeno, que en la especie, acorde a nuestro régimen legal, abordaremos dos tipos: autoridades de control y organismos garantes.

La diferencia en la denominación de las autoridades se debe a las diferencias en el régimen de tratamiento, puesto que, en el caso de autoridades de control, al recaer sus decisiones y resoluciones sobre tratamiento de particulares, su ámbito de actuación se encuentra limitado a los principios y procedimientos en la materia. Esta situación es distinta en el caso de los organismos garantes, pues corresponde a éstos la tutela directa de un derecho fundamental a través de mecanismos que constituyen verdaderos medios de control de la constitucionalidad, utilizando para tales efectos los que constituyen los derechos ARCO, o el *habeas data*.

Se considera necesario abordar el esquema de contrapesos por parte del Estado y las funciones dedicadas a la gestión de esta protección a través de dichas instituciones que, dados los requerimientos sociales de esta era digital, representan verdaderos bálsamos y a la vez baluartes para definir un mínimo de exigencias legales que impriman un imperativo ético a los hechos y efectos generados a partir del imperativo tecnológico. Estos contrapesos representan un conjunto de valores que encuentran su punto de equilibrio a través del respeto del derecho a la privacidad y se instrumenta en principio, a partir de la protección de datos personales.

Si bien la legislación mexicana en la materia establece, de manera implícita, los deberes inherentes a la continuidad en la protección de los datos personales a partir de la seguridad de la información en todos los supuestos que constituyen tratamiento (dentro y fuera de la organización a través de las transferencias), resulta necesario reconocer expresamente dicho principio de continuidad de nuestra legislación, puesto que el Reglamento Europeo de Protección de Datos ha dado pauta para tal efecto por medio de lo dispuesto en su artículo 44, que dice:

> Sólo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del

> presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Principio al cual el doctor Nelson Remolina Angarita ha denominado, en varias ocasiones, como principio de continuidad, el cual, en sustancia, implica que el responsable o encargado que transfiera datos deberá estar seguro que en el lugar de destino se mantenga o mejore el nivel de protección y los derechos del titular del dato, incluidas las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional, así como a la recolección de datos personales. Para tal efecto, podrá utilizar diversas alternativas como las cláusulas contractuales o normas corporativas vinculantes, a las cuales hace ya referencia el reglamento y que también puede ser expandible a los instrumentos de protección de datos personales de la ONU, la APEC y la OCDE, cuando se hace referencia a garantías comparables o protección equivalente.

Si bien los artículos 74 y 75 del RLFPDPPP previenen lo anterior en relación con las transferencias de datos personales, también dicha obligación de mejorar el nivel de protección se agota con el receptor sin considerar las ulteriores transferencias o la recolección internacional de datos personales, por lo que para que el principio de continuidad pueda cobrar vigencia, se estima conveniente incluir dichos elementos complementarios, es decir las subsecuentes transferencias.

A través de esta postura se advierte la necesidad de promover la cooperación internacional para una efectiva tutela y/o protección de los derechos en comento, a fin de hacer frente, como un esfuerzo conjunto y articulado de las instituciones, para asegurar el cumplimiento de dichos derechos en la era digital, en donde, de manera concreta, el internet juega un papel determinante, dado su modelo de gobernanza que escapa a la reglamentación de varios países.

Ante dicho escenario, existen importantes esfuerzos internacionales para cerrar brechas y estrechar lazos a fin de estar a la altura de este reto. Unas muestras de ello son la Conferencia Internacional de Comisionados de Privacidad y Protección de Datos, el Foro de Autoridades de Privacidad Asia–Pacífico y la Red Iberoamericana de Protección de Datos, a través de los cuales, año con año se generan iniciativas para hacer un frente común en la defensa de la protección de los datos personales y la privacidad.

Sobre el particular, se estima importante citar el documento generado con motivo de la 37 Conferencia Internacional de Comisionados de Privacidad y Protección de Datos Personales en Ámsterdam, Holanda, denominada *Privacy Bridges* (Puentes de Privacidad), la cual surgió como propuesta de solución frente al conflicto internacional que se suscitó a partir de la determinación de un nivel inadecuado de protección del mecanismo de intercambio de datos entre los Estados Unidos de Norteamérica y la Unión Europea, denominado *Safe Harbor* (Puerto Seguro), que ante la resolución emitida con motivo del caso *Europe vs. Facebook*, obligó a transitar a un nuevo mecanismo denominado *Privacy Shield* (Escudo de Privacidad).

A través de los puntos expuestos en los Puentes de Privacidad se plantearon, de manera integral, las necesidades de cooperación, exigencia de aplicación de la ley e investigación en torno a mecanismos homologados a nivel internacional para hacer frente a las necesidades de protección de los ciudadanos de los países miembros, a través de la supervisión de oficio que las autoridades en protección de datos personales deben realizar frente al tratamiento de los responsables.

En el caso de la Red Iberoamericana de Protección de Datos, destaca la adopción, en el año 2017, del documento Estándares de Protección de Datos Personales para los Estados Iberoamericanos, a través del cual se pretende brindar directrices homologadas a los países miembros, acordes con los más altos estándares contemporáneos internacionales.

Desde esta perspectiva, el papel que desempeñan las autoridades en protección de datos personales resulta fundamental para la salvaguarda de los derechos fundamentales reconocidos como tales en la corriente contemporánea de derechos humanos, sin perder de vista que la propia evolución social y económica, a la cual se enfrenta la humanidad, seguramente seguirá poniendo en entredicho los paradigmas existentes, en los cuales, eventualmente, el segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos podrá adquirir un nuevo significado, tanto para el sector público como para el privado.

En ese entendido, desde un punto de vista particular, el reconocimiento del derecho a la protección de datos personales a partir de la reforma del 1 de junio de 2009 es un acierto. Sin embargo, corresponde a las autoridades de protección de datos personales coadyuvar con la ciudadanía en su ejercicio y vigencia, a fin de que este derecho adquiera la dimensión efectiva para la tutela de los supuestos que pretende garantizar, lo cual va más allá de la mera instrumentación de la protección de datos personales, sino que abarca el derecho a ser feliz y a proteger los derechos intangibles de las personas, tal y

como Luis D. Brandeis y Samuel D. Warren concibieron en 1890 en su artículo *The Right to Privacy* (El derecho a la privacidad).

Finalmente, se considera importante señalar que el nivel de protección de datos personales en México ha avanzado de manera significativa y se encuentra en franca consolidación. El régimen de protección de datos personales en nuestro país va adquiriendo distintivos propios y el nivel de protección es equiparable al de los instrumentos jurídicos más avanzados, a pesar de que éstos se encuentran en continua revisión y actualización dada la dinámica social y económica.

Así, en el ámbito de los particulares, si bien nuestra primera aproximación con la protección de datos personales puede trazarse a partir de 2002 con la publicación de la Ley para Regular las Sociedades de Información Crediticia, no es sino ocho años después que, de manera concreta, a dicho régimen de protección se le atribuye contenido propio y no cuenta, siquiera, con una década de implementación.

No obstante, las autoridades involucradas con el régimen de particulares, el INAI y la Secretaría de Economía, han realizado esfuerzos considerables para asegurar la plena vigencia de la protección de datos personales en este sector, lo cual es digno de reconocimiento ante ciertas mediciones como el índice de privacidad en internet de Best VPN.org, en donde se sitúa a nuestro país en el grupo azul, que se traduce en cumplimiento medio/suficiente, pero que reconoce las fortalezas del régimen de protección de datos personales en México en un nivel adecuado en comparación con otros países.

En consecuencia, se estima que la decisión de asignarle al INAI las funciones como autoridad de control en protección de datos personales constituye un acierto que ha facilitado la asimilación rápida de la materia en nuestro sistema jurídico, permitiendo que un sólo organismo se especialice en el ámbito de protección, tanto del sector público como del privado. No obstante que el artículo transitorio 7 del 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, estableció, de manera expresa, la posibilidad de la creación de una autoridad de control independiente, como se observa a continuación:

> En tanto se determina la instancia responsable encargada de atender los temas en materia de protección de datos personales en posesión de particulares, el organismo garante que establece el artículo 6o. de esta Constitución ejercerá las atribuciones correspondientes.

Disposición que, al día de hoy, habilita al INAI como autoridad de control de protección de datos personales en posesión de los particulares, a pesar de que el artículo 3 fracción XI de la LFPDPPP sigue haciendo referencia al Instituto Federal de Acceso a la Información y Protección de Datos, al que hace alusión la abrogada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Correlaciones

Constitución y Leyes:
Constitución Política de los Estados Unidos Mexicanos.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el DOF el 26 de enero de 2017.
Ley Federal de Procedimiento Administrativo, publicada en el DOF el 4 de agosto de 1994.
Reglamentos y normatividad:
Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el DOF el 21 de diciembre de 2011.
Lineamientos del Aviso de Privacidad, publicados en el DOF el 17 de enero de 2013.
Recomendaciones en materia de seguridad de datos personales, publicadas en el DOF el 30 de octubre de 2013.
Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicados en el DOF el 17 de enero de 2013.
Parámetros de Autorregulación en materia de Protección de Datos Personales, publicados en el DOF el 29 de mayo de 2014.
Acuerdo mediante el cual se aprueban las reglas de uso del logotipo del Registro de Esquemas de Autorregulación Vinculante REA-INAI y condiciones para su autorización, publicado el 7 de abril de 2017.
Criterios judiciales:
Décima Época, registro: 2015161, instancia: Segunda Sala, tipo de Tesis: Aislada, fuente: Gaceta del Semanario Judicial de la Federación, Libro 46, septiembre de 2017, Tomo I, materia: Constitucional, tesis: 2a. CXLI/2017 (10a.), página: 777, rubro: “PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. EL ARTÍCULO 60, PÁRRAFO ÚLTIMO, DE LA LEY FEDERAL RELATIVA, NO VULNERA EL PRINCIPIO DE RESERVA DE LEY”.
Décima Época, registro: 2012350, instancia: Tribunales Colegiados de Circuito, tipo de Tesis: Aislada, fuente: Gaceta del Semanario Judicial de la Federación, Libro 33, agosto de 2016, Tomo IV, materia(s): Constitucional, tesis: I.9o.A.70 A (10a.), página: 2679, rubro: “PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. EL ARTÍCULO 116, FRACCIÓN VI,

DEL REGLAMENTO DE LA LEY FEDERAL RELATIVA, AL PREVER QUE A LA SOLICITUD DE PROTECCIÓN DE DERECHOS (ARCO) DEBERÁ ADJUNTARSE EL DOCUMENTO EN EL QUE EL PROMOVENTE SEÑALE "LAS DEMÁS PRUEBAS QUE OFREZCA", NO VIOLA EL PRINCIPIO DE RESERVA DE LEY".

Legislación comparada:

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).

Análisis de contenido

En función de las características de tratamiento en el régimen de los particulares, es dable referirnos al INAI como autoridad de control en la materia, no obstante, dada su vinculación con el ámbito económico y en los derechos de los consumidores, también se reconocen facultades a la Secretaría de Economía como autoridad reguladora, lo cual justifica la división del presente capítulo bajo análisis en dos secciones (ámbito de actuación de la autoridad de control y ámbito de actuación de las autoridades reguladoras) a fin de desarrollar los principios aplicables para cada supuesto.

a) Ámbito de actuación de la autoridad de control

El artículo 38 de la Ley establece, de manera general, que el INAI tendrá por objeto:

1. Difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana.
2. Promover el ejercicio de dicho derecho.
3. Vigilar la debida observancia de las disposiciones previstas en la Ley.

A partir de estos supuestos, se desarrollan las atribuciones del Instituto con las que pueden identificarse sus características como autoridad de control, mismas que se encuentran expresamente previstas en el artículo 39 de la LFPDPPP, disposición que, si bien previene en su fracción XII las "demás que le confieran esta Ley y demás ordenamientos aplicables", es dable señalar que el RLFPDPPP no establece un artículo en particular con el desdoblamiento de las atribuciones previstas en Ley, por lo que para su integración debe apegarse a la correlación entre las disposiciones del Reglamento y la Ley, atendiendo a los principios de jerarquía normativa y reserva de ley en lo que hace al régimen de particulares, y en una integración legal y/o ponderación en torno a otras disposiciones de tipo legal.

En ese contexto, es factible identificar las atribuciones como autoridad de control, en los supuestos siguientes:

I. Como autoridad de investigación, supervisión y sanción.

En esta hipótesis podemos identificar las fracciones I y VI del artículo 39 de la LFPDPPP relativas a vigilar y verificar el cumplimiento de las disposiciones contenidas en esta ley, en el ámbito de su competencia con las excepciones previstas por la legislación, así como conocer y resolver los procedimientos de protección de derechos y de verificación señalados en esta ley e imponer las sanciones según corresponda.

No obstante, sobre el particular, se estima necesario analizar lo establecido en el último párrafo de los artículos 45, 60 y 62 de la LFPDPPP que remiten hacia el RLFPDPPP y el desarrollo de los procedimientos, a través de los cuales el INAI vigila, verifica y sanciona el cumplimientode la Ley, que eventualmente pueden enfrentar un problema de constitucionalidad en materia de legalidad y seguridad jurídica.

Este tema que ha generado inquietud en el foro jurídico, cuyo testimonio se observa a partir del contenido de las tesis 2a. CXLI/2017, I.9o.A.70 A, de la décima época, publicadas en la *Gaceta del Semanario Judicial de la Federación*, en las cuales se denuncia la contravención al principio de reserva de ley, que en ambos supuestos, fueron determinados inexistentes. No obstante, a fin de determinar la contravención a este principio, es necesario determinar cuáles son las formalidades esenciales del procedimiento y, a partir de ahí, determinar la conformidad o no de las disposiciones de la LFPDPPP con los principios establecidos en los artículos 14, segundo párrafo y 16, primer párrafo de la Constitución federal. Para este efecto, es válido remitirse a lo dispuesto por la LFPA que establece las reglas del procedimiento administrativo común en materia federal.

Solamente atendiendo el grado de afectación con relación a los derechos humanos vulnerados sería posible identificar si existe inconstitucionalidad o no respecto estos supuestos y no simplemente porque la LFPDPPP remita al reglamento para su desarrollo.

Se estimó analizar este tópico en este apartado por identificarse dentro de los criterios que, hasta el momento, han sido generados por nuestro más alto tribunal, ya que si bien el Tribunal Federal de Justicia Administrativa ha producido tesis sobre la tramitación de dichos procedimientos, y el propio INAI ha difundido casos relevantes relacionados con su actuación, no se ha profundizado en el cumplimiento de los requisitos que deberían exigirle como autoridad de control, y que eventualmente, pudieran afectar el procedimiento, como en el caso de las visitas de verificación en materias, como la fiscal.

II. Como autoridad normativa o reguladora en la materia.

En este apartado, encontramos las fracciones II y IV del artículo 39 de la LFPDPPP relativas a interpretar en el ámbito administrativo la Ley, así como a emitir los criterios y recomendaciones de conformidad con las disposiciones aplicables de esta Ley para efectos de su funcionamiento y operación. A partir de estos supuestos, el INAI conduce las acciones por parte de los responsables del tratamiento de datos personales. Tal como se puede advertir, las atribuciones normativas del INAI como autoridad de control son limitadas a supuestos concretos, que a pesar de su particularidad son susceptibles de crear situaciones jurídicas específicas al desarrollar las disposiciones previstas en la LFPDPPP y su reglamento. Lo anterior, en comparación con las atribuciones normativas con las que cuenta como organismo garante nacional, como en el caso de las fracciones XIX, XXVII y XXVIII del artículo 89 de la LGPDPPSO, que le otorgan las atribuciones de emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general para el debido cumplimiento de los principios, deberes y obligaciones que establece dicha ley, así como para el ejercicio de los derechos de los titulares de emitir lineamientos generales para el debido tratamiento de los datos personales y para homologar el ejercicio de los derechos ARCO. Mediante esta acotación de atribuciones, los particulares cuentan con la certidumbre jurídica de que su esquema de cumplimiento se encuentra basado, sustancialmente, en los supuestos establecidos expresamente en la Ley.

De manera complementaria, el 30 de octubre de 2013 se publicaron en el *Diario Oficial de la Federación* las Recomendaciones en materia de seguridad de datos personales, a través del cual se brindan directrices para el cumplimiento del principio de responsabilidad y deber de seguridad en torno a los datos personales. En lo que hace al resto de los instrumentos normativos, como veremos más adelante, éstos se han desarrollado de manera conjunta con la Secretaría de Economía, a la cual, la LFPDPPP le otorga dicha atribución en coadyuvancia con el INAI.

III. Como autoridad consultora, asesora o preventiva.

Se estima que tiene tal carácter a partir de lo dispuesto por las fracciones III y X del artículo 39 de la LFPDPPP que previenen las atribuciones de proporcionar apoyo técnico a los responsables que lo soliciten para el cumplimiento de las obligaciones establecidas en la presente ley, así como elaborar estudios de impacto sobre la privacidad, previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes. El INAI cuenta con la atribución de fungir como ente consultor.

En lo que respecta al apoyo técnico, se aprecia que el INAI ha desarrollado herramientas que resultan útiles para facilitar el cumplimiento de la LFPDPPP como su reglamento y los lineamientos del aviso de privacidad, publicados en el DOF el 17 de enero de 2013, o el Generador de Avisos de Privacidad y el abc del aviso de privacidad que apoyan, de manera importante, a los responsables con la elaboración y redacción de dichos documentos de una manera sencilla, a través de una herramienta gratuita, a la cual pueden accederse en el apartado de protección de datos personales de la página de internet del INAI.

Así mismo, en 2014 se publicó la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, a través de la cual se establecen los requerimientos para el cumplimiento del principio de responsabilidad y la seguridad de datos personales basado en un esquema de sistemas de gestión.

De manera adicional, facilita datos de contacto para obtener asesoría telefónica, con lo cual se llega a compensar la falta de delegaciones u oficinas de representación del INAI en las entidades federativas, labor que sin duda todavía es una tarea pendiente, a fin de lograr presencia y sensibilización en todo el territorio mexicano, respecto a la importancia de implementar mecanismos de protección de datos personales.

Sin embargo, en lo que respecta a la atribución relativa a elaborar estudios de impacto sobre privacidad, con independencia de los alcances de la atribución, las evaluaciones de impacto a la privacidad o evaluaciones de impacto en la protección de datos, tratándose del ámbito de particulares, debe quedar como una obligación a cargo del responsable, en la cual podrá participar excepcionalmente la autoridad de control, pero no como una obligación.

En ambos supuestos, se observa que el INAI no ha facilitado los instrumentos para ello, ya sea de manera similar a la presentación de solicitudes de protección de derechos o denuncias a través de internet, en caso de que constituye un entregable de aquél o elaborando una guía que contenga los requisitos de este documento, a fin de que los responsables puedan formular estos estudios en los casos que se requiera dentro de su organización conforme lo establece la Ley.

IV. Como autoridad promotora, capacitadora y difusora del derecho a la protección de datos personales.

A partir de lo señalado en las fracciones V y XI, consistentes en divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos, las finalidades del tratamiento y las capacidades técnicas y económicas del responsable y, desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en posesión de los particulares y brindar capacitación a los sujetos obligados. De manera similar a lo señalado en el apartado anterior, el INAI ha desarrollado herramientas útiles para tal efecto.

Muestra de ello son el Vulnerómetro, el Corpus Iuris y el aula virtual de capacitación, así como las guías para titulares de datos personales (tradicional e interactiva), para prevenir el robo de identidad y para la configuración de privacidad en redes sociales, procedimiento para ejercer los derechos ARCO, así como recomendaciones que ayudan a mantener segura la privacidad y los datos personales en el entorno digital.

V. Como autoridad coadyuvante de otras autoridades.

Tomando como referencia las fracciones VII y IX del artículo 39 de la LFPDPPP, consistentes en la cooperación con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos, así como acudir a foros internacionales en el ámbito de dicha Ley. Esta vinculación y colaboración, que como se comentó en la introducción, resulta fundamental para que las autoridades en la materia puedan realizar una defensa efectiva de los ciudadanos. El INAI es miembro de la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, de la Red Iberoamericana de Protección de Datos y del Foro de Autoridades Asia-Pacífico.

VI. Como sujeto obligado.

En este último supuesto previsto por la fracción VIII del artículo 39 de la LFPDPPP consiste en rendir al Congreso de la Unión un informe anual de sus actividades, avances y retos relacionados con la protección de los datos personales en México.

b) Ámbito de actuación de las autoridades reguladoras

La sección segunda del presente capítulo establece las disposiciones relativas al marco regulatorio en materia de protección de datos personales. Esto es así, puesto que la materia bajo estudio se *transversaliza* dentro de las instituciones en el entendido de que, prácticamente, todos los procesos requieren el manejo de datos personales, y por ende, los requerimientos varían dependiendo de la naturaleza y contexto del tratamiento.

El artículo 40 de la LFPDPPP establece que esta Ley constituirá el marco normativo que las dependencias deberán observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda con la coadyuvancia del INAI, supuestos en los cuales se identifican, de manera enunciativa, las dependencias de la Administración Pública Federal como son las secretarías de Economía, Salud, Comunicaciones y Transportes, Hacienda y Crédito Público y Educación, pero también podría resultar aplicable para organismos autónomos como el Instituto Federal de Telecomunicaciones. A través de esta disposición se brinda unidad y coherencia al régimen de

protección de datos personales en posesión de particulares a partir de la LFPDPPP.

Los artículos 77 y 80 del RLFPDPPP establecen, dentro del Capítulo V, relativo a la coordinación entre autoridades, los elementos a considerar, como a continuación se observa:

> Emisión de regulación secundaria. Artículo 77. Cuando la dependencia competente, atendiendo a las necesidades que advierta sobre el sector que regule, determine la necesidad de normar el tratamiento de datos personales en posesión de los particulares podrá, en el ámbito de sus competencias, emitir o modificar regulación específica, en coadyuvancia con el Instituto. Asimismo, cuando el Instituto derivado del ejercicio de sus atribuciones advierta la necesidad de emitir o modificar regulación específica para normar el tratamiento de datos personales en un sector o actividad determinada, podrá proponer a la dependencia competente la elaboración de un anteproyecto.
> Mecanismos de coordinación. Artículo 78. Para la elaboración, emisión y publicación de la regulación a que se refiere el artículo 40 de la Ley, la dependencia y el Instituto establecerán los mecanismos de coordinación correspondientes. En todos los casos, la dependencia y el Instituto, en el ámbito de sus atribuciones, determinarán las disposiciones que normen el tratamiento de datos personales en el sector o actividad que corresponda.

No obstante lo anterior, la Secretaría de Economía se incluye, de manera particular, señalando que para efectos de esta Ley tendrá como función difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en el territorio mexicano, promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital y el desarrollo económico nacional en su conjunto.

Esto es así, puesto que uno de los principales supuestos de aplicación de la protección de datos personales es el económico, en el entendido de que los flujos de datos son necesarios para las operaciones que soportan las relaciones comerciales y económicas, la oferta y demanda de bienes y servicios, así como los derechos del consumidor.

Como parte de ello, el artículo 42 de la LFPDPPP establece que, en lo referente a las bases de datos de comercio, la regulación que emita la Secretaría de Economía, únicamente será aplicable a aquellas bases de datos automatizadas o que formen parte de un proceso de automatización, lo cual constituye una de las principales preocupaciones en el tratamiento de datos personales a través de medios digitales, en el entendido de que si su manejo inadecuado por parte de los responsables puede generar afectaciones graves a los titulares como discriminación, también su regulación deficiente

puede impactar, de manera directa, en la actividad económica, así como en la invención e innovación.

Los factores económicos y tecnológicos han impulsado el desarrollo de la protección de datos personales en posesión de los particulares en un mercado globalizado, en el cual resulta necesario contar con mecanismos de control homologados que permitan transacciones seguras, y por ello, a partir de las atribuciones de la Secretaría de Economía, se observan los principales supuestos sobre los que se abordan los esfuerzos en la materia.

En las fracciones I, II, VII, IX y X del artículo 43 de la LFPDPPP se hace referencia a la actividad promotora y difusora de la Secretaría de Economía pues promueve el conocimiento sobre la protección de los datos personales en el ámbito comercial, fomenta las buenas prácticas comerciales en materia de protección de datos personales, acude a foros comerciales nacionales e internacionales sobre protección de datos personales, o a eventos de naturaleza comercial, apoya la realización de actos que contribuyen en la difusión de la protección de los datos personales y celebra convenios con cámaras de comercio, asociaciones y organismos empresariales en materia de protección de datos personales.

Atendiendo a las razones señaladas con anterioridad, la Secretaría de Economía cuenta con una amplia variedad de atribuciones normativas, mismas que en su mayoría deben ser implementadas en coadyuvancia con el INAI, como las previstas por las fracciones III, IV, V y VIII del artículo 43 de la LFPDPPP, referentes a emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad, a que se refiere la presente ley, como emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general a que se refiere el artículo 40, fijar los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere el artículo 44 de la presente ley, incluido la promoción de normas mexicanas u oficiales en coadyuvancia con el INAI, diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y de las tecnologías de la información en materia de protección de datos personales.

Atribuciones a partir de las cuales se ha emitido la normatividad siguiente:

- Lineamientos del Aviso de Privacidad.
- Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

- Parámetros de Autorregulación en materia de Protección de Datos Personales.

Así mismo y de manera particular, se establece como atribución llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento, lo cual realiza la Procuraduría Federal del Consumidor a través del Registro Público para Evitar Publicidad (REPEP), anteriormente denominado Registro Público de Consumidores (RPC), constituyendo un mecanismo de protección a los consumidores a no ser molestados por los proveedores con publicidad.

Así, debemos realizar anotaciones puntuales respecto a los esquemas de autorregulación vinculante y los mecanismos de certificación, mismos que se encuentran regulados en el artículo 44 de la LFPDPPP y del 79 al 86 del RLFPDPPP. Esta figura establece que las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante, que complementen lo dispuesto por la presente ley. Dichos esquemas deberán incluir mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento. Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares. Dichos esquemas serán notificados de manera simultánea a las autoridades sectoriales correspondientes y al INAI.

El funcionamiento de dichos mecanismos se lleva a cabo en términos de lo dispuesto por el RLFPDPPP y de la normatividad señalada con anterioridad, así como por las disposiciones administrativas y formatos que el INAI genera, conformando un registro de esquemas de autorregulación vinculante.

El artículo 80 del RLFPDPPP establece los objetivos específicos de la autorregulación vinculante, como se observa a continuación:

> Objetivos específicos de la autorregulación
>
> Artículo 80. 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 y tendrán los siguientes objetivos primordiales:

I. Coadyuvar al cumplimiento del principio de responsabilidad al que refiere la Ley y el presente Reglamento.
II. Establecer procesos y prácticas cualitativos en el ámbito de la protección de datos personales que complementen lo dispuesto en la Ley.
III. Fomentar que los responsables establezcan políticas, procesos y buenas prácticas para el cumplimiento de los principios de protección de datos personales, garantizando la privacidad y confidencialidad de la información personal que esté en su posesión.
IV. Promover que los responsables de manera voluntaria cuenten con constancias o certificaciones sobre el cumplimiento de lo establecido en la Ley, y mostrar a los titulares su compromiso con la protección de datos personales;
V. Identificar a los responsables que cuenten con políticas de privacidad alineadas al cumplimiento de los principios y derechos en la Ley, así como de competencia laboral para el debido cumplimiento de sus obligaciones en la materia.
VI. Facilitar la coordinación entre los distintos esquemas de autorregulación reconocidos internacionalmente.
VII. Facilitar las transferencias con responsables que cuenten con esquemas de autorregulación como puerto seguro.
VIII. Promover el compromiso de los responsables con la rendición de cuentas y adopción de políticas internas consistentes con criterios externos, así como para auspiciar mecanismos para implementar políticas de privacidad, incluyendo herramientas, transparencia, supervisión interna continua, evaluaciones de riesgo, verificaciones externas y sistemas de remediación.
IX. Encauzar mecanismos de solución alternativa de controversias entre responsables, titulares y terceras personas, como son los de conciliación y mediación.

Estos esquemas serán vinculantes para quienes se adhieran a los mismos, la adhesión será de carácter voluntario.

También, el artículo 83 del RLFPDPPP establece que los esquemas de autorregulación vinculante podrán incluir la certificación de los responsables en materia de protección de datos personales, supuesto a través del cual se brinda una mayor certeza respecto al cumplimiento de objetivos de control en torno a la seguridad de la información vinculada con la protección de datos personales.

Así mismo, el contenido de los esquemas de autorregulación vinculante se encuentra estrechamente ligado con técnicas de seguridad de la información y modelos de sistemas de gestión que tienen como base el ciclo de mejora continua, círculo o ciclo de *Deming* o PHVA, que se basa en cuatro actividades principales que son: planear, hacer, verificar y actuar.

No obstante, el único incentivo previsto por el artículo 81 del RLFPDPPP es que cuando un responsable adopta y cumple un esquema de autorregulación, dicha circunstancia será tomada en consideración para determinar la atenuación de la sanción que corresponda, en caso de verificarse algún incumplimiento a lo dispuesto por la LFPDPPP y el RLFPDPPP por parte del INAI. Asimismo, el INAI podrá determinar otros incentivos para la adopción de esquemas de autorregulación, así como mecanismos que faciliten procesos administrativos ante él mismo.

Dado lo señalado en la introducción de esta colaboración, se aprecia que los esquemas de autorregulación vinculante son de suma importancia en la industria como mecanismos de responsabilidad demostrada de un adecuado tratamiento de datos personales. Sin embargo, como se apuntó también, la adopción de dichos esquemas va aparejado a un valor económico y, por ende, resulta necesario generar incentivos efectivos para su implementación.

Esto es así, puesto que, si bien se estima que la inclusión de esquemas de autorregulación vinculante constituye un importante impulso a la materia, también, dada la falta de objetivos claros y beneficios derivados de su adopción, no resulta atractivo para los particulares atendiendo cuando menos, dos factores:

- La falta de presencia del INAI en el sector, como autoridad de control sancionadora, con casos relevantes en la agenda nacional, ya que si bien es cierto que el propio Instituto ha dado cuenta de las multas impuestas con motivo de infracción de la LFPDPPPP, también lo es, que los responsables de tratamiento en las entidades federativas ven lejana la posibilidad o inclusive desconocen sus obligaciones como responsables en el tratamiento de datos personales. En consecuencia, ante la falta de sanción, el incentivo de adoptar esquemas de autorregulación vinculante a partir de la atenuante de la infracción se diluye. Aunado a ello, se observa contradictorio el hecho de que los entes que las adopten incumplan la LFPDPPP y su reglamento, puesto que en esencia dicho mecanismo, aplicado adecuadamente, disminuye de manera importante los riesgos inherentes al tratamiento de datos personales.

- La falta de claridad de los objetivos de la protección de datos que se persiguen a través de la adopción de estos esquemas, pues que no se precisa si su ámbito de aplicación es local, regional, nacional o internacional, así como sus equivalencias con otros sistemas de gestión, lo que provoca que los esquemas de autorregulación vinculante no representen una opción interesante para la industria, en función a los recursos que deben ser invertidos para su implementación.

Se considera que, en poco tiempo, la protección de datos personales y la privacidad constituirán diferenciadores y ventajas competitivas en la industria, por lo que las empresas adoptarán, cada vez más, mecanismos para su protección como respuesta a las demandas de sus consumidores. Sin embargo, esta reputación, por el momento, no es el incentivo que puede impulsar los esquemas de autorregulación vinculantes.

La figura de los esquemas de autorregulación vinculantes encuentra grandes similitudes con las normas corporativas vinculantes y con las certificaciones previstas por el Reglamento Europeo de Protección de Datos, pues constituyen mecanismos para facilitar las transferencias y están basados en supuestos distintos a las decisiones de adecuación, al considerarse garantías, como se observa a continuación:

Artículo 46
Transferencias mediante garantías adecuadas

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.
2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:
   a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
   b) normas corporativas vinculantes de conformidad con el artículo 47;
   c) cláusulas tipo de protección de datos adoptadas por la comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;
   d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;
   e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o
   f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.
3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o
b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.
5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Por ello, se estima que debe incentivarse la adopción de esquemas de autorregulación vinculante a través de la incorporación de un mayor contenido de interés para las empresas, que permita que las acciones implementadas en México puedan ser reconocidas en otros países, a fin de facilitar, en principio, el flujo de datos transfronterizos y a la vez facilitar el cumplimiento de las obligaciones por parte de responsables que realizan el tratamiento de datos personales a nivel internacional, para lo cual se requiere:

- Que el INAI gestione, a partir de su intervención en agrupaciones internacionales, mecanismos de cooperación y reconocimiento entre países con esquemas de autorregulación vinculante y/o normas corporativas vinculantes, a fin de que los responsables cuenten con la certidumbre de que sus procesos serán validados y reconocidos por las autoridades competentes a nivel internacional y que, por otra parte, estos esquemas o normas corporativas se adecuen a las necesidades de las organizaciones.
- Proponer y describir con precisión los tipos de esquemas de autorregulación vinculante y sus efectos, a fin de poder determinar los procedimientos adecuados para cada uno de ellos. En la inteligencia que un sello de confianza tiene un alcance más limitado que una certificación sobre un adecuado tratamiento de datos personales. A partir de ello, el INAI puede incrementar la cobertura de su supervisión y control de los particulares a través de la renovación de los certificados, entrega de informes periódicos por parte de los responsables y procedimientos análogos de revisión que permitan acreditar un entorno de control de responsables que se autorregulen, a fin de iniciar procedimientos a aquellos omisos.

- Reconocer mayores incentivos a los responsables que asumen un mayor nivel de compromiso o responsabilidad, estableciendo que no serán sujetos a verificaciones por parte del INAI durante el tiempo que el esquema de autorregulación y/o el certificado se mantenga vigente, salvo que hubiese denuncia en su contra o alguna vulneración de seguridad comprobada.
- Reconocer y homologar esquemas de autorregulación vinculante a partir de otros sistemas de gestión a través de los cuales se acredite que se está dando cumplimiento a la LFPDPPP, a través de lo cual, no solamente se flexibiliza su implementación por parte del responsable, sino que se reducen considerablemente los costos asociados y el desgaste de recursos.
- Determinar los tipos de responsables a los cuales les resulta recomendable implementar esquemas de autorregulación vinculante a partir del tipo de tratamiento, tamaño de la empresa, número de empleados, sensibilidad de los datos, entre otros.
- Mantener y consolidar vinculación en iniciativas exitosas tales como el reconocimiento de mejores prácticas en protección de datos personales.

Esto es así, ya que en caso de mantener el esquema aplicable actualmente ¿cuál es el valor añadido por parte de la certificación que no brinde un sistema de gestión de seguridad?, ¿por qué sería mejor implementar un esquema de autorregulación vinculante y no otra certificación en calidad o seguridad de la información?, ¿cómo puede asegurarse la conformidad de un esquema de autorregulación vinculante en comparación con un sistema de gestión de seguridad de información? y ¿un esquema de autorregulación vinculante podría desarrollarse a partir de una norma o sistema de gestión diverso?

Supuestos sobre los cuales el INAI y la Secretaría de Economía tienen mucho sobre lo cual avanzar si se pretende darle continuidad a la seguridad en el tratamiento de los datos personales.

Conclusiones

El papel de las autoridades en la protección de datos personales resulta fundamental para la custodia de los derechos y libertades de las personas en la actualidad.

El INAI cuenta con dos roles en su carácter de autoridad en materia de protección de datos personales, a saber: como organismo garante y como autoridad de control.

El artículo transitorio séptimo del 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, establece que el INAI mantendrá las atribuciones como autoridad de control en materia de protección de datos personales en posesión de los particulares de manera transitoria, en lo que se crea la autoridad correspondiente. Sin embargo, se estima que gran parte del avance que se ha tenido en nuestro país, se debe a dicha decisión, por lo que bastaría con que el INAI cuente con el presupuesto suficiente para llevar a cabo su función como autoridad de control y buscar una mayor presencia en las entidades federativas, sin dejar las estrategias relativas al uso de tecnologías y plataformas informáticas para incrementar el alcance de sus atribuciones.

Las características del INAI como autoridad de control pueden ser analizadas desde distintas vertientes, razón por la cual, solamente se abordaron supuestos generales que pueden resultar útiles en una valoración prospectiva, sin embargo, aunque no se pudo profundizar el estudio y/o el análisis particular del contenido de la LFPDPPP y su reglamento a fin de no aumentar la extensión de la colaboración, resulta evidente que la transformación dinámica que ha tenido la materia ha impactado con los temas que se encuentran en dicha legislación, por lo que si bien, el régimen normativo aplicable es consistente, congruente, coherente y por tanto vigente en comparación con los principales instrumentos internacionales, también lo es la Ley, su Reglamento y demás disposiciones que requieren modificaciones para actualizar conceptos, corregir errores y brindar contexto a las figuras contenidas, como en el caso de los procedimientos y los esquemas de autorregulación vinculante, a fin de que cumplan sus efectos y se ajusten a las previsiones constitucionales.

Los flujos de datos personales transfronterizos mediante transferencias o recolecciones internacionales de datos, así como la cooperación entre autoridades de control, deben insertarse, cada vez con más fuerza en nuestro entorno, a fin de que los datos personales puedan ser utilizados en beneficio de sus titulares de manera segura, para ello se estima necesario generar un entorno de continuidad en la protección.

Los mecanismos de autorregulación vinculantes pueden resultar de gran utilidad para el tratamiento responsable de datos personales. Sin embargo, se estima que dicha figura debe ser dotada de contexto y contenido, a fin de que resulte atractiva su implementación por parte de los responsables del tratamiento.

Por otra parte, también se advierte necesario dar mayor coherencia y transparencia a las disposiciones en materia de protección de datos personales en posesión de los particulares, ya que si bien el INAI en su página

de internet ofrece un apartado específico sobre este régimen, la experiencia de navegación y de usuario no es la mejor, aunado a que varios de los contenidos aquí apuntados no son accesibles de manera ágil, por lo que resultaría recomendable el desarrollo de un micrositio especializado o una oficina virtual que compense la falta de presencia física del INAI en las entidades federativas, facilitando el ejercicio de los derechos de los titulares, así como el cumplimiento de obligaciones por parte de los responsables, de una manera ágil, a través de un sitio que cuente con toda la información relacionada sobre el tema, organizada de manera inteligente y relacionando los supuestos de aplicación a través de enlaces.

La exigencia en el fortalecimiento de las autoridades de control en la materia se debe a que la dinámica de la sociedad demanda nuevos derechos que, conforme al contexto actual, en un futuro, eventualmente, podrán ser afectados por parte de empresas particulares que cuenten con un papel preponderante en el mercado, por lo que la protección de datos personales puede irse posicionando como ese derecho que pueda devolvernos la libertad y seguridad ante la infinidad de riesgos ante los cuales no encontramos expuestos ante el imperativo tecnológico de la sociedad de la información y el conocimiento.

Referencias

Gobierno de España. (2018). *Boletín Oficial del Estado*. Agencia Estatal. Recuperado de: *https://www.boe.es/*

Diario Oficial de la Unión Europea. (2016). *Reglamento General de Protección de Datos.* Recuperado de: *https://www.boe.es/doue/2016/119/L00001-00088.pdf*

APPA. (2018). *Asia Pacific Privacy Authorities.* Recuperado de: *http://www.appaforum.org/*

Cámara de Diputados H. Congreso de la Unión LXIV Legislatura. (2018). *Leyes Federales y reglamentos de Leyes Federales vigentes*. Recuperado de: *http://www.diputados.gob.mx/LeyesBiblio/*

Department of Commerce of United States of America. (2018). *Privacy Shield Framework*. Recuperado de: *https://www.privacyshield.gov/welcome*

INAI. (2018). *P*ágina de internet del I*NAI*. Recuperado de: *http://inicio.ifai.org.mx/SitePages/ifai.aspx*

ICDPPC. (2018). *International Conference of Data Protection and Privacy Commissioners.* Recuperado de: *https://icdppc.org/*

Massachusetts Institute of Technology. (2018). *Privacy Bridges EU–US Privacy Bridges*. Recuperado de: *https://privacybridges.mit.edu/*

Red Iberoamericana de Protección de Datos. (2018). *P*ágina de internet de la Red Iberoamericana de Protección de Datos. Recuperado de: *http://www.redipd.es/index-ides-idphp.php*

Warren, S y Brandeis, L. (1890, diciembre 15). “Right to Privacy”. *Harvard Law Review*. Vol. 4. No. 5. Pp. 193-220. Recuperado de: *http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf*

Secretaría de Gobernación. (2018). *Diario Oficial de la Federación.* Recuperado de: *https://www.dof.gob.mx/*

Suprema Corte de Justicia de la Nación. (2018). *Semanario Judicial de la Federación*. Recuperado de: *https://sjf.scjn.gob.mx/sjfsist/Paginas/tesis.aspx*

Tribunal Federal de Justicia Administrativa. (2018). *Sistema de Consulta de Tesis y Jurisprudencia.* Recuperado de: *http://sctj.tfjfa.gob.mx/SCJI/*

CAPÍTULO VII
DEL PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS

CAPÍTULO VII
DEL PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS

Artículo 45. *El procedimiento se iniciará a instancia del titular de los datos o de su representante legal, expresando con claridad el contenido de su reclamación y de los preceptos de esta Ley que se consideran vulnerados. La solicitud de protección de datos deberá presentarse ante el Instituto dentro de los quince días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable.*

En el caso de que el titular de los datos no reciba respuesta por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo de respuesta previsto para el responsable. En este caso, bastará que el titular de los datos acompañe a su solicitud de protección de datos el documento que pruebe la fecha en que presentó la solicitud de acceso, rectificación, cancelación u oposición.

La solicitud de protección de datos también procederá en los mismos términos 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, el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida.

Recibida la solicitud de protección de datos ante el Instituto, se dará traslado de la misma al responsable, para que, en el plazo de quince días, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que a su derecho convenga.

El Instituto admitirá las pruebas que estime pertinentes y procederá a su desahogo. Asimismo, podrá solicitar del responsable las demás pruebas que es-

time necesarias. Concluido el desahogo de las pruebas, el Instituto notificará al responsable el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días siguientes a su notificación.

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 Reglamento de la Ley establecerá la forma, términos y plazos conforme a los que se desarrollará el procedimiento de protección de derechos.

Artículo 46. *La solicitud de protección de datos podrá interponerse por escrito libre o a través de los formatos, del sistema electrónico que al efecto proporcione el Instituto y deberá contener la siguiente información:*

I. El nombre del titular o, en su caso, el de su representante legal, así como del tercero interesado, si lo hay;
II. El nombre del responsable ante el cual se presentó la solicitud de acceso, rectificación, cancelación u oposición de datos personales;
III. El domicilio para oír y recibir notificaciones;
IV. La fecha en que se le dio a conocer la respuesta del responsable, salvo que el procedimiento inicie con base en lo previsto en el artículo 50;
V. Los actos que motivan su solicitud de protección de datos, y
VI. Los demás elementos que se considere procedente hacer del conocimiento del Instituto.

La forma y términos en que deba acreditarse la identidad del titular o bien, la representación legal se establecerán en el Reglamento.

Asimismo, a la solicitud de protección de datos deberá acompañarse la solicitud y la respuesta que se recurre o, en su caso, los datos que permitan su identificación. En el caso de falta de respuesta sólo será necesario presentar la solicitud.

En el caso de que la solicitud de protección de datos se interponga a través de medios que no sean electrónicos, deberá acompañarse de las copias de traslado suficientes.

Artículo 47. *El plazo máximo para dictar la resolución en el procedimiento de protección de derechos será de cincuenta días, contados a partir de la fecha de presentación de la solicitud de protección de datos. Cuando haya causa justi-*

ficada, el Pleno del Instituto podrá ampliar por una vez y hasta por un período igual este plazo.

Artículo 48. *En caso que la resolución de protección de derechos resulte 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.*

Artículo 49. *En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere el artículo 46 de esta Ley, y el Instituto no cuente con elementos para subsanarlo, se prevendrá al titular de los datos dentro de los veinte días hábiles siguientes a la presentación de la solicitud de protección de datos, por una sola ocasión, para que subsane las omisiones dentro de un plazo de cinco días. Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de protección de datos. La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto para resolver la solicitud de protección de datos.*

Artículo 50. *El Instituto suplirá las deficiencias de la queja en los casos que así se requiera, siempre y cuando no altere el contenido original de la solicitud de acceso, rectificación, cancelación u oposición de datos personales, ni se modifiquen los hechos o peticiones expuestos en la misma o en la solicitud de protección de datos.*

Artículo 51. *Las resoluciones del Instituto podrán:*

I. Sobreseer o desechar la solicitud de protección de datos por improcedente, o
II. Confirmar, revocar o modificar la respuesta del responsable.

Artículo 52. *La solicitud de protección de datos será desechada por improcedente cuando:*

I. El Instituto no sea competente;
II. El Instituto haya conocido anteriormente de la solicitud de protección de datos contra el mismo acto y resuelto en definitiva respecto del mismo recurrente;
III. Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular que pueda tener por efecto modificar o revocar el acto respectivo;

IV. Se trate de una solicitud de protección de datos ofensiva o irracional, o
V. Sea extemporánea.

Artículo 53. *La solicitud de protección de datos será sobreseída cuando:*

I. El titular fallezca;
II. El titular se desista de manera expresa;
III. Admitida la solicitud de protección de datos, sobrevenga una causal de improcedencia, y
IV. Por cualquier motivo quede sin materia la misma.

Artículo 54. *El Instituto 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. La solicitud de protección de datos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.

Para efectos de la conciliación a que se alude en el presente ordenamiento, se estará al procedimiento que se establezca en el Reglamento de esta Ley.

Artículo 55. *Interpuesta la solicitud de protección de datos ante la falta de respuesta a una solicitud en ejercicio de los derechos de acceso, rectificación, cancelación u oposición por parte del responsable, el Instituto dará vista al citado responsable para que, en un plazo no mayor a diez días, acredite haber respondido en tiempo y forma la solicitud, o bien dé respuesta a la misma. En caso de que la respuesta atienda a lo solicitado, la solicitud de protección de datos se considerará improcedente y el Instituto deberá sobreseerlo.*

En el segundo caso, el Instituto emitirá su resolución con base en el contenido de la solicitud original y la respuesta del responsable que alude el párrafo anterior.

Si la resolución del Instituto a que se refiere el párrafo anterior determina la procedencia de la solicitud, el responsable procederá a su cumplimiento, sin costo alguno para el titular, debiendo cubrir el responsable todos los costos generados por la reproducción correspondiente.

Artículo 56. *Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.*

Artículo 57. *Todas las resoluciones del Instituto serán susceptibles de difundirse públicamente en versiones públicas, eliminando aquellas referencias al titular de los datos que lo identifiquen o lo hagan identificable.*

Artículo 58. *Los titulares que consideren que han sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento a lo dispuesto en la presente Ley por el responsable o el encargado, podrán ejercer los derechos que estimen pertinentes para efectos de la indemnización que proceda, en términos de las disposiciones legales correspondientes.*

COMENTARIO

Olivia Andrea Mendoza

Introducción

En este apartado analizaremos el capítulo VII de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) relativo al denominado Procedimiento de Protección de Derechos.

Este procedimiento está previsto en la legislación en materia de datos personales en posesión de los particulares, a fin de garantizar al titular de datos personales que haya formulado previamente una solicitud de derechos ARCO (acceso, rectificación, cancelación y oposición frente al tratamiento de datos personales) al responsable de dicho tratamiento, y no haya sido atendida, la posibilidad de un recurso legal de protección, ante la autoridad garante en la materia a nivel nacional. Es decir, ante la negativa o atención inadecuada de una solicitud de derechos ARCO formulada al responsable del tratamiento, resulta aplicable el procedimiento de protección de derechos, que analizaremos en las siguientes líneas.

Es importante decir que la autoridad garante del derecho a la protección de datos personales en México es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), quien deberá conocer las solicitudes de inicio del procedimiento de protección de derechos, respecto de la no atención o inadecuada respuesta de las solicitudes de derechos ARCO formuladas por los titulares de datos personales a personas físicas o morales de carácter privado, establecidas o que presten sus servicios en México[138] y que lleven a cabo tratamiento de datos personales.[139]

[138] De acuerdo con el transitorio quinto de la LFPDPPP, en cumplimiento a lo dispuesto por el artículo tercero transitorio del decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el *Diario Oficial de la Federación* el 30 de abril de 2009, las disposiciones locales en materia de protección de datos personales en posesión de los particulares se abrogan, y se derogan las demás disposiciones que se opongan a la LFPDPPP. Este transitorio fue previsto en esos términos, ya que en su momento existieron algunas legislaciones estatales en materia de protección de datos personales en posesión de particulares, lo cual complicaba el cumplimiento por parte de las empresas, ya que tendrían que adecuar sus tratamientos, de conformidad a la entidad de la República en la que prestaran sus servicios o estuvieran establecidos. Esto evidentemente frenaba la competitividad y el cumplimiento en la materia, por lo que, a partir de las facultades del Congreso de la Unión para legislar en materia de datos personales en posesión de particulares, se optó por una legislación federal única, de aplicación a todo el país.

[139] En términos del artículo 2 de la LFPDPPP, son sujetos regulados por esta Ley los particulares que sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos

Correlaciones

Del artículo 113 al 127 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Análisis de contenido

De acuerdo con el artículo 45 de la LFPDPPP, el procedimiento de protección de derechos inicia a instancia del titular de los datos o de su representante legal, y para tal efecto, deberán expresar con claridad el contenido de su reclamación y de los preceptos de la Ley que se consideran vulnerados.[140] El término para presentar la solicitud de protección de derechos es de hasta 15 días[141] siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable respecto de la solicitud de derechos ARCO.[142] Esta disposición refiere particularmente al ejercicio de los denominados derechos ARCO (acceso, rectificación, cancelación y oposición) frente al tratamiento de datos personales.[143]

En este sentido, previo a la solicitud del procedimiento de protección de derechos, se deberá cuidar no haber incurrido en algunas de las causales que tendrían por no presentadas las solicitudes iniciales de derechos ARCO. Un ejemplo de esto se encuentra previsto en el artículo 94 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), el cual establece algunos requerimientos mínimos, por ejemplo, en el caso de solicitudes de acceso a datos personales, señala que, en la solicitud de acceso, para efectos de comunicar la respuesta, se deberá indicar el domicilio o cualquier otro medio para que sea notificada. En caso de no cumplir con este requisito, el responsable tendrá por no presentada la solicitud, dejando constancia de ello.

---

personales, con excepción de: las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y 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.

140 A pesar de dicha disposición, al tratarse de un derecho humano y bajo la interpretación del principio *pro persona* y a la naturaleza ciudadana del órgano garante del derecho a la protección de datos personales en México, aplica la suplencia de la queja, a favor de los titulares de datos personales. Esta afirmación ha quedado ya salvaguardada de manera expresa tanto en la LFPDPPP, como en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

141 De acuerdo con el artículo 5 de la LFPDPPP, a falta de disposición expresa en dicha Ley, se aplicarán de manera supletoria las disposiciones del Código Federal de Procedimientos Civiles y de la Ley Federal de Procedimiento Administrativo, por lo que el plazo referido para solicitar un procedimiento de Protección de Derechos, se computará de acuerdo con los días hábiles.

142 En términos del artículo 3, fracción XIV de la LFPDPPP, el responsable es la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

143 A partir de 2017, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados reconoce la "portabilidad" como una manifestación adicional, de los tradicionalmente reconocidos derechos ARCO. No obstante, a pesar de ser incluso un derecho recogido en el Reglamento General de Protección de Datos Europeo, no existe obligación expresa en la Ley, que obligue a garantizar la portabilidad de datos personales en posesión de particulares; es decir, en México ha quedado como una obligación para los responsables o sujetos obligados primordialmente del sector público y no así para los responsables en el sector privado.

Causales del procedimiento de protección de derechos

En el caso de que el titular de los datos no reciba respuesta por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo de respuesta previsto para el responsable.[144] En este caso, bastará que el titular de los datos acompañe a su solicitud de protección de derechos el documento que pruebe la fecha en que presentó la solicitud de acceso, rectificación, cancelación u oposición.[145]

La solicitud del procedimiento de protección de derechos, también procede en los mismos términos cuando:

1. El responsable no entregue al titular los datos personales solicitados.[146]
2. El responsable entregue los datos personales solicitados en un formato incomprensible.[147]

---

144 De acuerdo con el artículo 32 de la LFPDPPP, el responsable deberá comunicar al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta. Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

145 De acuerdo con el artículo 124 del RLFPDPPP, en caso de que el procedimiento se inicie por falta de respuesta del Responsable a una solicitud de ejercicio de los derechos ARCO, el INAI correrá traslado al responsable para que, en su caso, acredite haber dado respuesta a la misma, o bien, a falta de ésta, emita la respuesta correspondiente y la notifique al titular con copia al Instituto, en un plazo de 10 días contados a partir de la notificación. En caso de que el responsable acredite haber dado respuesta a la solicitud de ejercicio de derechos en tiempo y forma, y haberla notificado al titular o su representante, el procedimiento de protección de derechos será sobreseído por quedar sin materia.

146 De acuerdo con el artículo 34 de la LFPDPPP, el responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos:

I. Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;
II. Cuando en su base de datos, no se encuentren los datos personales del solicitante;
III. Cuando se lesionen los derechos de un tercero;
IV. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y
V. Cuando la rectificación, cancelación u oposición haya sido previamente realizada.

La negativa a que se refiere este artículo podrá ser parcial, en cuyo caso, el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular. En todos los casos anteriores, el responsable deberá informar el motivo de su decisión y comunicarla al titular, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes.

147 De acuerdo con el artículo 45 de la LFPDPPP, "la solicitud de protección de datos también procederá en los mismos términos 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, el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida".

3. El responsable se niegue a efectuar modificaciones o correcciones a los datos personales.[148]
4. El titular no esté conforme con la información entregada por considerar que está incompleta o que no corresponde a la información requerida.

Las causales de procedencia del procedimiento de protección de derechos, también se encuentran previstas en el artículo 115 del RLFPDPPP, el cual señala que el mismo se verificará cuando exista una inconformidad por parte del titular, derivada de acciones u omisiones del responsable con motivo del ejercicio de los derechos ARCO cuando:

I. El titular no haya recibido respuesta por parte del responsable.

II. El responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible.

III. El responsable se niegue a efectuar las rectificaciones a los datos personales.

IV. El titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción.

V. El responsable se niegue a cancelar los datos personales.

VI. El responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, no quiera atender la solicitud de oposición.

VII. Por otras causas que a juicio del INAI sean procedentes conforme a la LFPDPPP o el RLFPDPPP.

[148] El artículo 26 de la LFPDPPP señala las excepciones del derecho de cancelación de datos personales. Es decir, el responsable no estará obligado a cancelar datos personales de solicitudes formuladas cuando:
I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento.
II. Deban ser tratados por disposición legal.
III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular.
V. Sean necesarios para realizar una acción en función al interés público.
VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular.
VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

Requisitos de la solicitud de protección de datos

Por su parte, el artículo 46 de la LFPDPPP señala los requisitos que debe contener la solicitud de protección de datos, la cual podrá interponerse por escrito libre o por medio de los formatos del sistema electrónico que al efecto proporcione el INAI, deberá contener la siguiente información:

I. El nombre del titular o, en su caso, el de su representante legal, así como del tercero interesado, si lo hay.

II. El nombre del responsable ante el cual se presentó la solicitud de acceso, rectificación, cancelación u oposición de datos personales.

III. El domicilio para oír y recibir notificaciones.

IV. La fecha en que se le dio a conocer la respuesta del responsable, salvo que el procedimiento inicie con base en la falta de respuesta por parte del responsable.

V. Los actos que motivan su solicitud de protección de datos.

VI. Los demás elementos que se considere procedente hacer del conocimiento del Instituto.

El procedimiento de protección de datos deberá ir acompañado de la solicitud y la respuesta que se recurre o, en su caso, los datos que permitan su identificación. En el caso de falta de respuesta solo será necesario presentar la solicitud.

El RLFPDPPP también señala los requisitos de la solicitud de protección de derechos e incluye disposiciones adicionales respecto de las pruebas ofrecidas a fin de demostrar las afirmaciones del titular del dato personal. El artículo 116 del citado ordenamiento dice que el “promovente” deberá adjuntar a su solicitud de protección de derechos la información y los documentos siguientes:

I. Copia de la solicitud del ejercicio de derechos que corresponda, así como copia de los documentos anexos para cada una de las partes, de ser el caso.

II. El documento que acredite que actúa por su propio derecho o en representación del titular.

III. El documento en que conste la respuesta del responsable, de ser el caso.

IV. En el supuesto en que impugne la falta de respuesta del responsable, se deberá acompañar de una copia con el acuse o constancia de recepción de la solicitud del ejercicio de derechos por parte del responsable.

V. Las pruebas documentales que ofrece para demostrar sus afirmaciones.

VI. El documento en el que señale las demás pruebas[149] que ofrezca.

VII. Cualquier otro documento que considere procedente someter a juicio del Instituto.

Si el titular no pudiera acreditar que acudió con el responsable, ya sea porque éste negó a recibir la solicitud de ejercicio de derechos ARCO o a emitir el acuse de recibido, lo hará del conocimiento del Instituto mediante un escrito y le dará vista al responsable para que manifieste lo que a su derecho convenga, a fin de garantizar al titular el ejercicio de sus derechos ARCO.

El artículo 50 de la LFPDPPP señala que el INAI suplirá las deficiencias de la queja en los casos que así se requiera, siempre y cuando no altere el contenido original de la solicitud de acceso, rectificación, cancelación u oposición de datos personales, ni se modifiquen los hechos o peticiones expuestos en la misma o en la solicitud de protección de datos. Es decir, adquiere relevancia, de nueva cuenta el principio *pro persona* en la dimensión de la salvaguarda del derecho a la protección de datos personales.

Acreditación de la personalidad

En relación con los documentos que acrediten al titular de los datos personales o de su representante legal, el artículo 96 del RLFPDPPP señala en el apartado: Requerimiento de Información Adicional, que en el caso de que el responsable no le requiera al titular documentación adicional para la acreditación de su identidad o de la personalidad de su representante, se entenderá por acreditada con la documentación aportada por el titular desde la presentación de su solicitud.

Derivado de esta disposición, resulta fundamental que el responsable, una vez que recibe la solicitud de derechos ARCO, revise la adecuada acreditación

[149] En términos del artículo 119 del RLFPDPPP, los medios de prueba que pueden ofrecerse son:
I. La documental pública;
II. La documental privada;
III. La inspección, siempre y cuando se realice a través de la autoridad competente;
IV. La presuncional en su doble aspecto, legal y humana;
V. La pericial;
VI. La testimonial, y
VII. Las fotografías, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología.
En caso de que se ofrezca prueba pericial o testimonial, se precisarán los hechos sobre los que deban versar y se señalarán los nombres y domicilios del perito o de los testigos, exhibiéndose el cuestionario o el interrogatorio respectivo en preparación de las mismas. Sin estos señalamientos se tendrán por no ofrecidas dichas pruebas.

de personalidad con los documentos que acompañan a la solicitud, ya que, si durante la etapa de atención de derechos ARCO no se da cuenta de que los documentos acompañados no demuestran la personalidad del titular o resultan confusos, si se entregan los datos personales sin haber hecho el requerimiento adicional de información en los plazos de ley,[150] dañaría el derecho a la protección de datos personales de un tercero, quien podría ser el verdadero titular de la información de carácter personal. Este ejemplo podría dar pauta a otro tipo de reparaciones del daño causado por parte del responsable en términos de la legislación del derecho civil.

El artículo 89 del RLFPDPPP establece que la acreditación de la identidad del titular de datos personales se hace a través de la presentación de la copia del documento de identificación y habiendo exhibido el original para su cotejo. También podrán ser admisibles los instrumentos electrónicos por medio de los cuales sea posible identificar fehacientemente al titular, u otros mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias, o aquéllos previamente establecidos por el responsable. La utilización de firma electrónica avanzada o del instrumento electrónico que lo sustituya eximirá de la presentación de la copia del documento de identificación. En el caso de representantes legales, deberán acreditar: a) la identidad del titular, b) la identidad del representante y c) la existencia de la representación mediante un instrumento público o una carta poder firmada ante dos testigos, o una declaración en comparecencia personal del titular.

En el caso de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, por ley se observarán las reglas de representación dispuestas en el Código Civil Federal.

En relación con el procedimiento de protección de derechos, el artículo 113 del RLFPDPPP señala que el INAI podrá tener por reconocida la identidad del titular o la personalidad del representante cuando ya hubiere sido acreditada ante el responsable al ejercer su derecho ARCO.

Medios para presentar la solicitud de procedimiento de protección de derechos

Respecto al sistema electrónico del INAI con la finalidad de solicitar el procedimiento de protección de derechos, el 23 de abril de 2018 se publicó en el *Diario Oficial de la Federación* el acuerdo mediante el cual se aprueba la modificación que establece el sistema electrónico para la

[150] De acuerdo con el artículo 96 del RLFPDPPP, el responsable podrá requerir al titular, por una vez y dentro de los cinco días siguientes a la recepción de la solicitud, que aporte los elementos o documentos necesarios para dar trámite a la misma. El titular contará con 10 días para atender el requerimiento, contados a partir del día siguiente en que lo haya recibido. De no dar respuesta en dicho plazo, se tendrá por no presentada la solicitud correspondiente.

presentación de solicitudes de protección de derechos y denuncias, así como la sustanciación de los procedimientos previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado el 28 de noviembre de 2013 y cuyo objeto actual es establecer las bases para la presentación y sustanciación de solicitudes de protección de derechos, denuncias que formulen los particulares, así como la sustanciación del procedimiento de imposición de sanciones a través del sistema electrónico del Instituto denominado IFAI-Prodatos, de conformidad con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y de la normatividad que de ésta deriva.[151]

En el mismo sentido, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en sus artículos 90 y 91, señala que las solicitudes de derechos ARCO pueden presentarse a través de los medios establecidos en el aviso de privacidad, los cuales pueden ser remotos o locales de comunicación electrónica,[152] y si hubiere algún servicio de atención al público específico para atender dichas solicitudes, tendrán que respetar los plazos establecidos para dar respuesta a las peticiones de derechos ARCO (máximo 20 días, contados desde la fecha en que se recibió la solicitud de derechos ARCO y pudiéndose ampliar dicho plazo una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso).

De nueva cuenta, en el artículo 92 del RLFPDPPP se establece una disposición en términos del principio *pro persona*, al señalar que cuando las disposiciones aplicables a determinadas bases de datos o tratamientos establezcan un procedimiento específico para solicitar el ejercicio de los derechos ARCO, se estará a lo dispuesto en aquéllas que ofrezcan mayores garantías al titular, y no contravengan las disposiciones previstas en la Ley.

En el caso de que la solicitud de protección de datos se interponga a través de medios que no sean electrónicos, deberá acompañarse de las copias de traslado suficientes.

El artículo 114 del RLFPDPPP establece que la solicitud de protección de derechos podrá presentarse en el domicilio del INAI, en sus oficinas habilitadas, por correo certificado con acuse de recibo o en el sistema del que hablamos previamente. En este último caso, siempre que el particular cuente con la certificación del medio de identificación electrónica a que se refiere el

[151] Acuerdo disponible en: *http://www.dof.gob.mx/nota_detalle.php?codigo=5520378&fecha=23/04/2018.* Fecha de consulta: 20 de septiembre de 2018.

[152] Cuando el promovente presente su solicitud por medios electrónicos, se entenderá que acepta que las notificaciones le sean efectuadas por dicho sistema o a través de otros medios electrónicos, salvo que señale un medio distinto para efectos de las notificaciones.

artículo 69-C de la Ley Federal de Procedimiento Administrativo, respecto de los expedientes electrónicos empresariales u otras disposiciones legales aplicables. En todo caso, se entregará al promovente un acuse de recibo en el cual conste, de manera fehaciente, la fecha de la presentación de la solicitud.

Cuando la solicitud sea presentada por el titular o su representante en la oficina habilitada por el Instituto, ésta hará constar la acreditación de la identidad o, en su caso, de la personalidad del representante, y podrá enviar o registrar por medios electrónicos, tanto la solicitud, como los documentos exhibidos. En este caso, la solicitud se tendrá por recibida cuando el Instituto, a través de ese mismo medio, genere el acuse de recibo correspondiente.

Lo anterior ocurre sin perjuicio de que la oficina habilitada remita al Instituto por correo certificado la constancia de identidad del titular o el documento de acreditación de la personalidad del representante, así como la solicitud y los documentos anexos para su integración al expediente respectivo. En el caso de que el titular envíe la solicitud y sus anexos por correo certificado, el plazo de recepción empezará a contar a partir de la fecha que conste en el sello de recepción del Instituto.

Admisión de solicitud de procedimiento de protección de derechos

Una vez que es presentada la solicitud de procedimiento de protección de derechos, de conformidad con el artículo 117 del RLFPDPPP, el INAI deberá acordar la admisión de la solicitud de protección de derechos en un plazo no mayor de 10 días a partir de su recepción. Acordada la admisión, el INAI notificará al promovente y correrá traslado al responsable, en un plazo no mayor de 10 días, anexando copia de todos los documentos que el titular hubiere aportado, a efecto de que manifieste lo que a su derecho convenga en un plazo de 15 días a partir de la notificación, debiendo ofrecer las pruebas que considere pertinentes.

Por su parte, el artículo 118 del RLFPDPPP señala que las pruebas deberán admitirse o desecharse mediante un acuerdo emitido por el INAI, y de ser necesario, serán desahogadas en una audiencia, de la cual se notificará el lugar o medio, la fecha y la hora a las partes.

Conciliación

Es interesante la figura de la conciliación dentro del procedimiento de protección de derechos contenida en el artículo 54 de la LFPDPPP, al señalar que el INAI podrá, en cualquier momento del procedimiento, buscar una conciliación entre el titular de los datos y el responsable, y de llegarse a un

acuerdo de conciliación entre ambos, se hará constar por escrito y tendrá efectos vinculantes. La solicitud de protección de datos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.

Esta misma etapa conciliatoria está prevista en el artículo 120 del RLFPDPPP y debe seguirse una vez admitida la solicitud de conformidad con el siguiente procedimiento:

I. En el acuerdo de admisión de la solicitud de protección de derechos, el INAI requerirá a las partes que manifiesten, por cualquier medio, su voluntad de conciliar, en un plazo no mayor a diez días contados a partir de la notificación de dicho acuerdo, mismo que contendrá un resumen de la solicitud de protección de datos personales y de la respuesta del responsable, si la hubiere, señalando los elementos comunes y los puntos de controversia. La conciliación podrá celebrarse presencialmente por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine dicho Instituto. En cualquier caso, la conciliación habrá de hacerse constar por el medio que permita acreditar su existencia.[153]

II. Aceptada la posibilidad de conciliar por las partes, el INAI señalará el lugar o medio, día y hora para la celebración de una audiencia de conciliación, la cual deberá realizarse dentro de los veinte días siguientes en que dicho Instituto haya recibido la manifestación de la voluntad de conciliar de las partes, en la que se procurará avenir los intereses entre el titular y el responsable. El conciliador podrá, en todo momento, requerir a las partes que presenten en un plazo máximo de cinco días, los elementos de convicción que estime necesarios para la conciliación. El conciliador podrá suspender cuando lo estime pertinente (o a instancia de ambas partes) la audiencia de conciliación hasta en dos ocasiones. En caso de que se suspenda la audiencia, el conciliador señalará día y hora para su reanudación. De toda audiencia de conciliación se levantará el acta respectiva, en la que conste el resultado de la misma. En caso de que el responsable o el titular o sus respectivos representantes no firmen el acta, ello no afectará su validez, debiéndose hacer constar dicha negativa.

[153] Se exceptúa de la etapa de conciliación, cuando el titular sea menor de edad y se haya vulnerado alguno de los derechos contemplados en la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, vinculados con las disposiciones en materia de datos personales, salvo que cuente con representación legal debidamente acreditada.

III. Si alguna de las partes no acude a la audiencia de conciliación y justifica su ausencia en un plazo de tres días, será convocado a una segunda audiencia. En caso de que no acuda a esta última, se continuará con el procedimiento de protección de derechos. Cuando alguna de las partes no acuda a la audiencia deconciliación sin justificación alguna, se continuará con el procedimiento.

IV. De no existir acuerdo en la audiencia de conciliación, se continuará con el procedimiento de protección de derechos.

V. En caso de que en la audiencia se logre la conciliación, el acuerdo deberá constar por escrito y tendrá efectos vinculantes y señalará, en su caso, el plazo de su cumplimiento.

VI. El cumplimiento del acuerdo dará por concluido el procedimiento de protección de derechos, en caso contrario, el INAI reanudará el procedimiento. El plazo máximo para que el INAI dicte resolución en el procedimiento de protección de derechos será suspendido durante el periodo de cumplimiento del acuerdo de conciliación.

De acuerdo con el artículo 54 de la LFPDPPP y el artículo 120 del RLFPDPPP, 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. La solicitud de protección de datos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.

Pruebas dentro del procedimiento de protección de derechos

Una vez que es recibida la solicitud de protección de datos ante el INAI, se dará traslado de la misma al responsable, para que, en el plazo de 15 días hábiles, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que a su derecho convenga.

El INAI admitirá las pruebas que estime pertinentes y procederá a su desahogo. Asimismo, podrá solicitar del responsable las demás pruebas que estime necesarias. Concluido el desahogo de las pruebas, el INAI notificará al responsable el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días siguientes a su notificación.

Audiencia

El artículo 45 de la LFPDPPP señala que, para los efectos del debido desahogo del procedimiento, el INAI resolverá sobre la solicitud de protección de datos formulada, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, como pueden ser aquellos que deriven de las audiencias que celebren con las partes.

En este sentido, el artículo 121 del RLFPDPPP manifiesta que el INAI determinará, en su caso, el lugar o medio, fecha y hora para la celebración de la audiencia referida en el párrafo anterior, la cual podrá posponerse sólo por causa justificada. En dicha audiencia se desahogarán las pruebas que por su naturaleza así lo requieran y se levantará el acta correspondiente.

Presentación de alegatos

Una vez que se haya dictado el acuerdo que tenga por desahogadas todas las pruebas, de conformidad con el artículo 122 del RLFPDPPP, se pondrán las actuaciones a disposición de las partes, para que éstos, en caso de quererlo, formulen alegatos en un plazo de cinco días, contados a partir de la notificación del acuerdo a que se refiere este artículo. Al término de dicho plazo se cerrará la instrucción y el INAI emitirá su resolución en el plazo máximo de 50 días, contados a partir de la fecha de presentación de la solicitud de protección de datos y en caso de causa justificada, se podrá ampliar por una vez y hasta por un período igual este plazo.[154]

Tercero interesado

De acuerdo con el artículo 123 del RLFPDPPP, en caso de que no se haya señalado tercero interesado, éste podrá apersonarse en el procedimiento mediante escrito en el que acredite interés jurídico para intervenir, hasta antes del cierre de instrucción. Deberá adjuntar a su escrito el documento en el que se acredite su personalidad cuando no actúe en nombre propio y las pruebas documentales que ofrezca.

[154] Artículo 47 de la LFPDPPP.

Tipos de resoluciones derivadas del procedimiento de protección de derechos

El artículo 51 de la LFPDPPP señala los sentidos de las resoluciones que puede emitir el INAI:

I. sobreseer o desechar la solicitud de protección de datos por improcedente, o

II. confirmar, revocar o modificar la respuesta del responsable.

El artículo 52 de la LFPDPPP señala que la solicitud de protección de datos será desechada por improcedente cuando:

I. El Instituto no sea competente.

II. El Instituto haya conocido anteriormente de la solicitud de protección de datos contra el mismo acto y resuelto en definitiva respecto del mismo recurrente.

III. Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular que pueda tener por efecto modificar o revocar el acto respectivo.

IV. Se trate de una solicitud de protección de datos ofensiva o irracional.

V. Sea extemporánea.

El artículo 53 de la LFPDPPP establece las causales de sobreseimiento, cuando:

I. El titular fallezca.

II. El titular se desista de manera expresa.

III. Admitida la solicitud de protección de datos, sobrevenga una causal de improcedencia.

IV. Por cualquier motivo quede sin materia la misma. Ejemplo de ello podría ser haber alcanzado algún acuerdo en la etapa conciliatoria mencionada previamente.

En este sentido, el artículo 124 del RLFPDPPP señala que en caso de que el responsable acredite haber dado respuesta a la solicitud de ejercicio de derechos en tiempo y forma, y haberla notificado al titular o su representante, el procedimiento de protección de derechos será sobreseído por quedar sin materia. Asimismo, cuando el responsable acredite haber dado respuesta a la

solicitud de ejercicio de derechos en tiempo y forma, y la solicitud de protección de derechos no haya sido presentada por el titular en el plazo que establece la Ley y el presente Reglamento, el procedimiento de protección de derechos se sobreseerá por extemporáneo. En caso de que la respuesta sea emitida por el responsable durante el procedimiento de protección de derechos o hubiere sido emitida fuera del plazo de 20 días o su respectiva ampliación, el responsable notificará dicha respuesta al INAI y al titular, para que este último, en un plazo de 15 días contados a partir de la notificación, manifieste lo que a su derecho convenga, a efecto de continuar el curso del procedimiento. Si el titular manifiesta su conformidad con la respuesta, el procedimiento será sobreseído por quedar sin materia.

Por su parte, el artículo 125 del RLFPDPPP señala que las resoluciones del INAI deberán cumplirse en el plazo y términos que las mismas señalen, y podrán instruir el inicio de otros procedimientos previstos en la Ley. Por ejemplo, en el caso del derecho de protección de datos personales en posesión de sujetos obligados, si la resolución emitida por el órgano garante señala un incumplimiento a las disposiciones en la materia, y dicha omisión fue cometida por un servidor público, puede darse vista al órgano de control interno correspondiente, a fin de iniciar el procedimiento administrativo respectivo. En materia de protección de datos personales en el sector privado, incluso la misma legislación aplicable reconoce la existencia de delitos en materia de datos personales, por lo que podrían derivar diversas autoridades competentes.

De acuerdo con el artículo 48 de la LFPDPPP, en caso que la resolución de protección de derechos resulte favorable al titular de los datos, se requerirá al responsable para que, en el plazo de 10 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 INAI dentro de los siguientes 10 días.

De acuerdo con el artículo 57 de la LFPDPPP, todas las resoluciones del Instituto serán susceptibles de difundirse públicamente en versiones públicas, eliminando aquellas referencias al titular de los datos que lo identifiquen o lo hagan identificable; es decir, se deberán generar versiones públicas de las mismas, salvaguardando la confidencialidad de los datos personales.

Medios de impugnación

De acuerdo con los artículos 56 de la LFPDPPP y 126 del RLFPDPPP, contra la resolución al procedimiento de protección de derechos procede el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

Al ser el derecho de protección de datos personales un derecho humano, una vez que se hubieren agotado las instancias nacionales reconocidas como competentes en la salvaguarda del mismo se podría acudir a la Comisión Interamericana de Derechos Humanos (CIDH), para que, de ser el caso y dictaminarse que se trata de una violación a ellos, pudiera dar participación a la CIDH, cuya jurisprudencia es vinculante para el Estado mexicano, siempre que sus disposiciones resultaran más favorables a las personas, de acurdo a la contradicción de tesis 293/2011.[155]

Reconducción del procedimiento

De acuerdo al artículo 127 del RLFPDPPP, en caso de que la solicitud de protección de derechos no actualice alguna de las causales de procedencia de dicho procedimiento y más bien al de verificación,[156] ésta se turnará a la unidad administrativa competente, en un plazo no mayor a diez días, contados a partir del día en que se recibió la solicitud.

Indemnización

De acuerdo con el artículo 58 de la LFPDPPP, cuando los titulares de datos personales consideren que han sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento a lo dispuesto en la legislación en materia de datos personales por parte del responsable o encargado del tratamiento de datos, podrán ejercer los derechos que estimen pertinentes para efectos de la indemnización que proceda. Ejemplo de ello podrían ser las acciones que, desde el derecho del consumidor o el derecho civil, se tienen previstas, a fin de compensar el daño o repararlo respectivamente.

Conclusiones

Como hemos podido observar a lo largo de este comentario al capítulo de la ley relativo al procedimiento de protección de derechos, cobra capital importancia el órgano garante de los derechos ARCO, los cuales ven de manera manifiesta su concreción cuando se materializa su protección en la resolución emitida por el INAI respecto a su vivencia en las organizaciones. Cobra especial relevancia el momento en que el titular del derecho acude al responsable y éste no cumple o cumple de manera incorrecta en la protección del ejercicio de los derechos

[155] Contradicción de tesis disponible en: *http://207.249.17.176/Transparencia/Epocas/Pleno/DecimaEpoca/293-2011-PL%20CT%20Ejecutoria.pdf* Fecha de consulta 20 de septiembre de 2018.

[156] Este procedimiento consiste en la facultad del INAI de requerir al responsable la documentación necesaria que acredite el cumplimiento de las disposiciones previstas en la legislación en materia de datos personales o en la regulación que de ella derive, así como realizar visitas en el establecimiento en donde se encuentren las bases de datos respectivas.

ARCO, pues es justo ahí donde germina la posibilidad de acudir a solicitar la fuerza del Estado para una debida protección.

Referencias

Acuerdo por el que se establece el sistema electrónico para la presentación de solicitudes de protección de derechos y de denuncias, así como la sustanciación de los procedimientos previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado el 28 de noviembre de 2013. Recuperado de: *http://dof.gob.mx/nota_detalle.php?codigo=5323658&fecha=28/11/2013*

Acuerdo mediante el cual se aprueba la modificación del diverso Acuerdo por el que se establece el sistema electrónico para la presentación de solicitudes de protección de derechos y de denuncias, así como la sustanciación de los procedimientos previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado el 28 de noviembre de 2013. Recuperado de: *http://www.dof.gob.mx/nota_detalle.php?codigo=5520378&fecha=23/04/2018*

Constitución Política de los Estados Unidos Mexicanos.

Contradicción de Tesis 293/2011 de la Suprema Corte de Justicia de la Nación. Disponible en: *http://207.249.17.176/Transparencia/Epocas/Pleno/DecimaEpoca/293-2011-PL%20CT%20Ejecutoria.pdf*

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

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

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

CAPÍTULO VII
DEL PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS

CAPÍTULO VIII
DEL PROCEDIMIENTO DE VERIFICACIÓN

Artículo 59. *El Instituto verificará el cumplimiento de la presente Ley y de la normatividad que de ésta derive. La verificación podrá iniciarse de oficio o a petición de parte.*

La verificación de oficio procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos a que se refiere el Capítulo anterior o se presuma fundada y motivadamente la existencia de violaciones a la presente Ley.

Artículo 60. *En el procedimiento de verificación el Instituto tendrá acceso a la información y documentación que considere necesarias, de acuerdo a la resolución que lo motive.*

Los servidores públicos federales estarán obligados a guardar confidencialidad sobre la información que conozcan derivada de la verificación correspondiente.

El Reglamento desarrollará la forma, términos y plazos en que se sustanciará el procedimiento a que se refiere el presente artículo.

COMENTARIO

Miguel Ángel Flores Guerrero

Introducción

Durante el proceso de análisis, discusión y aprobación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPP) en 2010, uno de los temas más discutidos fue la designación del órgano

garante, quien —a partir de su entrada en vigor— se encargaría de atender las quejas ciudadanas, así como de verificar el cumplimiento de los principios de protección de datos personales, recomendando medidas preventivas e incluso correctivas dirigidas a los responsables del tratamiento.

En este punto, las diversas iniciativas que se habían presentado desde el año 2001 (la primera del diputado federal Miguel Barbosa Huerta, integrante del grupo parlamentario del PRD del 6 de septiembre de ese año), tenían posturas radicalmente distintas sobre la autoridad o autoridades que debían ser investidas con las facultades de control y vigilancia de este derecho. Por ejemplo, la iniciativa presentada por el diputado federal Adolfo Mota Hernández del PRI, el 11 de diciembre de 2008, señalaba que la Secretaría de Economía era el organismo que contaba con una verdadera vocación para asegurar un adecuado balance entre los derechos de los particulares y, al mismo tiempo, para poder considerar las necesidades de la actividad industrial y comercial de nuestro país. Existían otras iniciativas como la que presentó el diputado federal Luis Gustavo Parra Noriega del PAN, el 4 de noviembre de 2008, que pretendían la creación de una nueva autoridad administrativa: la Comisión Nacional de Protección de Datos Personales, cuya naturaleza sería la de un organismo descentralizado de la administración pública federal, no sectorizado, dotado de personalidad jurídica y patrimonio propio, que con plena autonomía técnica y de gestión, pudiese dictar sus resoluciones. Incluso, dentro de aquellos proyectos que ya señalaban al Instituto Federal de Acceso a la Información Pública (IFAI)[157] como la posible autoridad de control, había iniciativas como la del diputado federal Jesús Martínez Álvarez de Convergencia, propuesta el 12 de enero de 2005, que contemplaban la creación de un nuevo órgano dentro del Instituto, conformado por tres comisionados, que realizarían funciones de supervisión, vigilancia y registro de bases de datos.

Si bien es cierto que cada una de las iniciativas contó con argumentos sólidos sobre la conveniencia de su modelo, los legisladores se vieron obligados a tomar en consideración criterios sobre la viabilidad financiera que implicaría la designación del órgano garante.

En este sentido, la comisión de presupuesto y cuenta pública de la Cámara de Diputados señaló que la creación de un nuevo organismo descentralizado como el propuesto por el diputado Gustavo Parra impactaría negativamente las finanzas públicas, dado su costo de implementación, por lo que se descartó la idea de crear una Comisión Nacional de Protección de Datos Personales.

[157] Denominado actualmente Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) a partir de la entrada en vigor de la Ley General de Transparencia y Acceso a la Información Pública, dada a conocer en el *Diario Oficial de la Federación* el 4 de mayo de 2015.

De esta forma, con la finalidad de evitar gastos e inversiones importantes que sobrevendrían con la creación de una nueva autoridad en materia de protección de datos personales, el legislativo decidió designar como autoridad de control, supervisión y vigilancia al IFAI, considerando que se necesitarían menos recursos para adecuar la estructura de este instituto para ejercer sus nuevas atribuciones en esta materia y aunado a otras ventajas como: la unificación de criterios (entre la transparencia y la protección de datos personales), una menor curva de aprendizaje, la autonomía ya consolidada del instituto y el posicionamiento con el que ya contaba el IFAI en el entorno político y social.

Correlaciones

Constitución Política de los Estados Unidos Mexicanos.
Ley Federal del Procedimiento Administrativo.
Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (del artículo 128 al artículo 139)
Ley General de Transparencia y Acceso a la Información Pública.
Ley Federal de Transparencia y Acceso a la Información Pública.
Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), 1980.
Marco de privacidad del Foro de Cooperación Económica Asia-pacífico (APEC), 2004.
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, 2016.
Resolución ACT-PRIV/21/02/2018.03.01.14, expediente INAI.3S.07.02 079/2017 de la Dirección General de Investigación y Verificación del Sector Privado.

Análisis de contenido

Una vez designada la autoridad en materia de protección de datos personales, comenzó la valoración sobre la conveniencia de que el Instituto tuviera, a la vez, las funciones de: órgano garante y de autoridad verificadora, o si sería más conveniente que la verificación del cumplimiento recayese en otra instancia, judicial o administrativa, para evitar que en algún momento dado el IFAI se pudiese convertir en juez y parte.

Durante esta valoración, uno de los puntos más importantes a considerar fue si esta autoridad de control (IFAI) u otras instancias reguladoras ya existentes como juzgados, procuradurías o comisiones que ya vigilaban este tema dentro de sus sectores (como la Procuraduría Federal del Consumidor, Profeco y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios

Financieros, Condusef), podrían verificar eficientemente el cumplimiento de los principios y derechos tutelados por esta norma.

Fue así que, el principal reto al que se enfrentaron legisladores, académicos, especialistas y representantes de los diferentes sectores (bancario, asegurador, tecnologías de información, internet, mercadotecnia, consumo y autoservicio entre otros) consistió en definir la naturaleza del proceso mediante el cual, con base en el mandato constitucional,[158] actuaría el ente verificador con poderes de investigación y correctivos para la aplicación de la legislación que se estaba desarrollando, sin que dichas facultades supusieran, por un lado, un exceso de trámites burocráticos con un alto costo para el Estado, y por otro, un proceso tan complejo que desmotivase al ciudadano a hacer valer sus derechos frente a la autoridad encargada de dicha vigilancia.

En este sentido, la primera parte de la discusión sobre el procedimiento de verificación se centró en determinar cuál sería la vía más eficiente y que sirviera como una medida provisoria e incluso precautoria[159] y a su vez fuera un medio resarcitorio en caso de que, vulnerado el derecho a la protección de datos personales de un titular, se debiera indemnizar el daño causado y prevenir alguna violación futura.

Como consecuencia de esta problemática, durante las rondas de discusiones, se definieron claramente dos posturas sobre cómo se pensaba debía ser regulado este procedimiento de verificación: la primera, que podemos denominar "tradicional", representada por aquellos que consideraban que la vía más eficiente era la jurisdiccional, en la que la verificación se realizara como parte de un procedimiento ordinario ante la justicia federal, muy a la manera de un habeas data,[160] evitando así que el propio IFAI tuviera las dos funciones: la de resolver procedimientos de protección de derechos y de ejecutar procedimientos de verificación, y la segunda, a la que podemos denominar "moderna", donde se pensó en aprovechar la experiencia e independencia del IFAI, para implementar un procedimiento de carácter administrativo por medio del cual se iniciasen las revisiones, a instancia de la misma autoridad, para determinar los posibles incumplimientos a las resoluciones dictadas con motivo de los procedimientos de protección de derechos a los que se refiere la Ley en

[158] El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos establece, en su segundo párrafo, que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley.

[159] Refiriéndonos a este concepto en el sentido más amplio que hay en derecho como aquellas medidas tendientes a garantizar el cumplimiento de una norma, o en su caso, encaminadas a asegurar la reparación de un posible daño.

[160] Es decir, como una acción procesal mediante la cual los tribunales constatasen el tratamiento legítimo de los datos personales y a través del cual el titular pudiese pedir una investigación sobre el tratamiento de su información.

su capítulo VII,[161] así como cuando la propia autoridad de protección de datos presumiera la existencia de violaciones a este derecho humano protegido por nuestra Carta Magna.

Dentro de los muchos factores que entraron en debate entre la conveniencia de estos mecanismos, se valoró que la saturación bajo la cual se encontraba el sistema judicial mexicano, aunado a la poca cultura jurídica que existía (y aún existe) en nuestro país de no acudir a hacer valer sus derechos frente a los tribunales,[162] haría de la vía jurisdiccional un mecanismo poco eficaz para el desarrollo de este procedimiento, por lo que fue descartada.

Del otro lado, la existencia de un organismo como el IFAI, que al momento de la discusión ya contaba con una base sólida y experiencia como autoridad verificadora en la parte de transparencia y acceso a la información pública gubernamental, permitió resaltar las ventajas fácilmente cuantificables que tenía como: la organización y estructura del propio Instituto que permitía un desarrollo menos burocrático de este procedimiento por la vía administrativa, aunado a que los ciudadanos identificaban ya esta autoridad como un ente establecido para la protección y salvaguarda de sus derechos.

De esta forma, el capítulo VIII de la Ley fue decantándose a favor de la idea de que el IFAI, además de encargarse de resolver los procedimientos de protección de derechos (como órgano de control), supervisara también, mediante facultades de investigación y medidas correctivas el cumplimiento de los principios y obligaciones contemplados en esta normatividad (como órgano de verificación), y que asimismo, pudiese ofrecer un asesoramiento especializado en la aplicación de los principios de la protección de los datos personales a los ciudadanos gracias a su bagaje de conocimientos y experiencia.

Sin embargo, el hecho de que el IFAI, por una parte fuera la autoridad encargada de resolver los procedimientos de protección de derechos y por la otra el encargado de ejecutar los procesos de verificación, generó la preocupación de que descuidase su rol como autoridad de protección de datos y se constituyese como un sistema policial que burocratizaría excesivamente la supervisión de este derecho, por lo que los trabajos se concentraron en sentar las bases para que la Ley, a través de un capítulo específico, delimitara la procedencia y alcance de la verificación.

[161] Procedimiento de protección de derechos iniciado a instancia del titular de los datos o su representante legal, cuando éste presuma que ha existido una violación a los principios de tratamiento de los datos establecidos en la ley en comento.

[162] De acuerdo con el documento denominado *Perspectivas Económicas 2018*, elaborado por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de forma conjunta con la Comisión Económica para América Latina y el Caribe de las Naciones Unidas (CEPAL) y el Banco de Desarrollo de América Latina, en colaboración con la Comisión Europea, la confianza de los mexicanos en el sistema judicial y en los tribunales es de apenas 32 por ciento, situándolo por debajo de los promedios de América Latina, el Caribe y de los países miembros de la OCDE.

En este sentido, si bien es cierto que las reglas supranacionales que se consideraron para la creación de esta Ley[163] aportaron en su momento normas y mecanismos relacionados con los principios de protección de datos personales, todas ellas dejaban al arbitrio de cada país desarrollar los mecanismos legislativos, judiciales o administrativos para verificar el cumplimiento de este derecho, sin entrar a fondo en la sustanciación, por lo que fue necesario recurrir a la experiencia de los procedimientos administrativos existentes en otras leyes en nuestro país. De esta manera, quedó definido dentro del texto legal, como atribución del IFAI, conocer y resolver los procedimientos de verificación, junto con la facultad de resolver los procedimientos de protección de derechos, así como la de imponer las sanciones que se pudieran derivar del incumplimiento de los mismos[164] y se procedió a sentar las bases de su tramitación en el capítulo VIII de la Ley.

Inicio del procedimiento de verificación

Conforme a lo señalado en el artículo 59, el inicio de la verificación administrativa en materia de protección de datos personales puede darse de dos formas: de oficio o a petición de parte. Estos supuestos fueron diseñados considerando la necesidad de que las atribuciones de vigilancia del Instituto no se circunscribieran únicamente a aquellos casos en los que se generara una denuncia por parte de algún titular de la información, sino también en aquellos casos en los que se manifestaran situaciones en las que la vulneración a los principios señalados en la norma fuera evidente o que las circunstancias justificaran legalmente investigar más a fondo alguna situación precisamente por tratarse de una garantía constitucional de los gobernados. Un ejemplo muy claro de esto fue el caso de Cambridge Analytica, en dónde esta empresa obtuvo, a través de una minería de información y de medios fraudulentos, datos personales de más de 87 millones de usuarios de la red social Facebook, utilizándolos para crear perfiles psicológicos con la finalidad de manipular e influenciar su toma de decisiones. En este caso, el Instituto inició una investigación para comprobar si existían incumplimientos a la Ley por parte de aquellas empresas en México que pudieran estar involucradas en los hechos relacionados con el citado caso.[165]

[163] Entre ellas las más importantes: (i) El Convenio 108 del Consejo de Europa, sobre protección de datos personales del 1 de octubre de 1985, la recomendación de la Organización para la Cooperación y el Desarrollo Económico (OCDE) en la que se contienen las directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales, adoptada el 23 de septiembre de 1980; y, (ii) los principios emitidos por el Foro de Cooperación Económica Asia-Pacífico (APEC) en su Marco de Privacidad del 2004.

[164] Dichas atribuciones se encuentran comprendidas en el artículo 39, fracción VI de la Ley en comento.

[165] INAI. (2018, abril 9). *Inicia INAI investigación de oficio por caso Cambridge Analytica*. Recuperado de: *http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-095-18.pdf*

En este sentido, las reglas establecidas en este capítulo de la Ley no dejan a la discrecionalidad pura o a una interpretación arbitraria de la autoridad el inicio de las verificaciones de oficio, sino que éstas se darán al cumplirse alguna de las dos hipótesis señaladas en el artículo 59.

La primera de estas hipótesis se cumple cuando, una vez concluido el procedimiento de protección de derechos al que se refiere el capítulo VII de la Ley, existe un incumplimiento en cuanto a lo proveído por la autoridad de protección de datos personales, es decir, exista una especie de desacato, entendido como una falta hacia la autoridad del órgano garante pues se desconoce su dignidad como guardián del bien jurídico tutelado: la protección de los datos personales. Por ejemplo, cuando el Instituto ordena a una empresa (responsable)[166] dar acceso a los datos que resguarda de un trabajador, dentro de un plazo determinado, y el sujeto obligado se niega a conceder dicho acceso o a entregar la información a su titular o cuando el INAI exige la eliminación de un registro y la organización responsable se niega a borrarla.

La segunda se cumple cuando existe la presunción fundada de posibles violaciones a la norma y sus principios, como en el caso Cambridge Analytica antes citado, o como en el oficio emitido por la Dirección General de Procedimientos de la Subprocuraduría de Servicios de la Profeco,[167] por medio del cual la procuraduría hizo del conocimiento del INAI la existencia de diversas páginas de internet a través de las cuáles se realizaba el tratamiento de datos personales y que, presuntamente, no contaban con avisos de privacidad, hecho que motivó el inicio de procedimientos de verificación de oficio por parte del Instituto, para investigarlo.

Estos supuestos permiten que el procedimiento de verificación iniciado de "oficio", no quede ligado a criterios meramente subjetivos de la autoridad de control, sino que en un caso su inicio se detona por el incumplimiento probado de la resolución al procedimiento de protección de derechos, y en el otro se genera por la existencia probada de hechos sobre los cuales se presume una posible vulneración a un derecho humano universalmente reconocido y garantizado en la constitución, situación en donde la Ley y el mandato constitucional son los preceptos legales que fundan el procedimiento; mientras que los hechos ocurridos (como la investigación de la Profeco o el incidente de Cambridge Analytica), son la causa directa tomada en cuenta para la realización de esta investigación (motivación).

[166] De acuerdo con el artículo 3, fracción XIV de la Ley en comento como la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

[167] Oficio PFC/SPS/DGP/0787/2017, emitido por la Dirección General de Procedimientos de la Subprocuraduría de Servicios de la Procuraduría Federal del Consumidor, notificado al INAI el 22 de junio de 2017.

En cuanto al inicio del procedimiento a petición de parte, al que se refiere el artículo 59, es importante aclarar que tampoco se trata de un proceso discrecional o subjetivo, en donde la simple presentación de la acusación o escrito de denuncia, es causa suficiente para su inicio, sino que requerirá que el denunciante sea capaz de aportar elementos que le permitan al Instituto fundar y motivar la revisión, pero además requerirá que los hechos denunciados no se encuentren ligados con el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, pues éstos son materia del procedimiento de protección de derechos. Por ejemplo, un procedimiento de verificación a petición de parte no procede si un titular basa su denuncia en que solicitó la cancelación de sus datos personales a una empresa y ésta no atendió su petición, pero si procederá si el quejoso señala en su petición que sus datos fueron recabados por una empresa a través de un formulario en una página de internet, en la cual no pudo encontrar un aviso de privacidad disponible para dicho tratamiento.

Por lo que toca a las facultades para que el Instituto lleve a cabo el procedimiento, este capítulo, en su artículo 60, buscó sentar las bases para que la autoridad pudiese allegarse de los elementos necesarios para evaluar si existe o no alguna infracción a los principios y obligaciones establecidos para la protección de los datos personales de los titulares, dentro de las cuales se incluyen: tanto documentos, como información[168] que, además de facilitar la inspección, permitan que el sujeto o persona moral investigada tenga la oportunidad de desvirtuar las presuntas violaciones a la norma por medio de las pruebas que pueda aportar coadyuvando a la investigación.

En otras palabras, el acceso que el Instituto podrá tener a la información y documentos, permite que la parte acusada pueda aportar también documentos, informes y hechos a su favor, respetándose así su garantía de audiencia. Ahora bien, en este mismo orden de ideas, en el ejercicio de esta atribución para la investigación de los hechos que motivaron el procedimiento de verificación, la autoridad de protección de datos personales, deberá, a su vez, tomar todas las previsiones para que los funcionarios públicos, a través de los cuales se realice este proceso, además de contar con las facultades expresas para llevar a cabo estas investigaciones y visitas de verificación, se encuentren también capacitados para recolectar la información y documentos resguardándolos confidencialmente, de manera que los revisores y visitadores que ejecutan este procedimiento, además de su investidura, estarán sujetos por Ley a una obligación de confidencialidad, lo que implica que toda la información y documentos que recaben durante sus visitas, no podrán ser utilizados para objetivos o finalidades que no estén expresamente previstos en la orden

[168] Entendida en el sentido más amplio como todos los datos y pruebas referentes a los hechos que motivaron la revisión de la autoridad.

de visita, dónde se enunciarán los hechos que motivan la verificación y los fundamentos de la misma.

Por lo que toca a la forma, términos y plazos en que se sustancia el procedimiento de verificación, los legisladores estimaron pertinente que las reglas fueran desarrolladas más tarde en la legislación secundaria, es decir, en el reglamento de la Ley, para así contar con un periodo adicional de tiempo para su desarrollo y evitar demoras en las discusiones y aprobación de la Ley en 2010. Así, uno de los grandes referentes para el desarrollo de este nuevo procedimiento lo proveyó la Ley Federal del Procedimiento Administrativo,[169] la cual, en su capítulo 11, señala las reglas para el desarrollo del procedimiento por el que se comprueba el cumplimiento de las disposiciones legales y reglamentarias aplicables a los actos, procedimientos y resoluciones de la administración pública federal centralizada. De tal forma que, con base en el procedimiento de verificación administrativa fue desarrollada la sustanciación del procedimiento de verificación en materia de protección de datos personales en el capítulo IX del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el *Diario Oficial de la Federación* el 21 de diciembre del 2011.

Conclusiones

Como se ha expuesto en este comentario, el procedimiento de verificación establecido en la Ley obedece a las exigencias que la vida moderna demanda para la efectiva salvaguarda de la protección de los datos personales. El propio Consejo de Europa en su reglamento (UE) 2016/679 el 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),[170] resalta actualmente la importancia que tiene cuidar que la autoridad de control de cada país tenga las facultades y la competencia para desempeñar sus funciones de forma independiente, incluyendo la de examinar las reclamaciones presentadas por un interesado, la realización de investigaciones sobre la aplicación de las normas y el fomento de la sensibilización del público acerca de los riesgos, las disposiciones, las garantías y los derechos en relación con el tratamiento de los datos personales.[171] En este capítulo, la Ley se asegura de que, en el ámbito de su competencia, la autoridad nacional

[169] El artículo 5 de la Ley señala que, a falta de alguna disposición expresa en su texto, se aplicarán, de forma supletoria, las disposiciones del Código Federal de Procedimientos Civiles y de la Ley Federal del Procedimiento Administrativo, por lo que esta última se erigió como un claro referente para la creación y coordinación del procedimiento de verificación previsto en este capítulo.

[170] El cual entró en vigor para toda la Unión Europea el 25 de mayo de 2018.

[171] Consideración (122) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y su la libre circulación.

de protección de datos personales cumpla con los criterios y parámetros de acción reconocidos y recomendados mundialmente en esta materia.

Además, las reglas establecidas en este capítulo permiten que sea a través de las etapas de un procedimiento de verificación, que estos exámenes o investigaciones no se realicen a través de criterios ambiguos o decisiones arbitrarias, sino que se proteja este derecho humano (reconocido universalmente) por medio de resoluciones que, de manera fundada y motivada, permitan a los involucrados la aportación de pruebas y argumentos de defensa en concordancia con la garantía de audiencia que tiene todo gobernado en nuestro país. Así se da un equilibrio entre la potestad que ejerce el Instituto como órgano de control constitucional de este derecho humano y los derechos de los investigados de aportar y alegar aquello que a su derecho convenga, lo que ha permitido hasta ahora el funcionamiento eficaz de este procedimiento.

Referencias

Cámara de Diputados. Dictamen de la comisión de gobernación con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del capítulo II del título segundo de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, del 13 de abril de 2010.

Cámara de Senadores. Minuta proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del capítulo II, del título segundo de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, aprobado en esta fecha por la Cámara de Diputados del H. Congreso de la Unión el 15 de abril de 2010.

OCDE/CAF/CEPAL. (2018). *Perspectivas económicas de América Latina 2018: Repensando las instituciones para el desarrollo*. París. OCDE. Recuperado de: *http://dx.doi.org/10.1787/leo-2018-es*

CAPÍTULO IX
DEL PROCEDIMIENTO DE IMPOSICIÓN DE SANCIONES

CAPÍTULO IX
DEL PROCEDIMIENTO DE IMPOSICIÓN DE SANCIONES

Artículo 61. *Si con motivo del desahogo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto, éste tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de esta Ley, iniciará el procedimiento a que se refiere este Capítulo, a efecto de determinar la sanción que corresponda.*

Artículo 62. *El procedimiento de imposición de sanciones dará comienzo con la notificación que efectúe el Instituto al presunto infractor, sobre los hechos que motivaron el inicio del procedimiento y le otorgará un término de quince días para que rinda pruebas y manifieste por escrito lo que a su derecho convenga. En caso de no rendirlas, el Instituto resolverá conforme a los elementos de convicción de que disponga.*

El Instituto admitirá las pruebas que estime pertinentes y procederá a su desahogo. Asimismo, podrá solicitar del presunto infractor las demás pruebas que estime necesarias. Concluido el desahogo de las pruebas, el Instituto notificará al presunto infractor el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días siguientes a su notificación.

El Instituto, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, resolverá en definitiva dentro de los cincuenta días siguientes a la fecha en que inició el procedimiento sancionador. Dicha resolución deberá ser notificada a las partes.

Cuando haya causa justificada, el Pleno del Instituto podrá ampliar por una vez y hasta por un período igual este plazo.

El Reglamento desarrollará la forma, términos y plazos en que se sustanciará el procedimiento de imposición de sanciones, incluyendo presentación de pruebas y alegatos, la celebración de audiencias y el cierre de instrucción.

COMENTARIO

Nuhad Ponce Kuri

Introducción

Toda norma jurídica es una regla imperativa de conducta, cuya violación genera la consecuencia de una posible imposición de sanción por parte del órgano del Estado que sea competente para ello.

La finalidad de una norma jurídica es ser efectiva para organizar y regular la convivencia pacífica de un grupo social, es por ello que cuenta con los mecanismos necesarios para garantizar su cumplimiento por medio de sanciones.

La sanción tiene la finalidad específica de regular las conductas de los individuos conforme a los preceptos que se establecen en el orden social. Una sanción es un efecto derivado del incumplimiento de una norma jurídica.

En caso de que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que es el órgano constitucional autónomo encargado de la transparencia y la protección de datos personales, tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de la Ley, se iniciará el procedimiento de imposición de sanciones para determinar y aplicar la sanción que corresponda.

Correlaciones

Artículos 140 al 144 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

Análisis de contenido

Las obligaciones de los responsables[172] en el tratamiento de datos personales son:

[172] Artículo 3, fracción XIV de la LFPDPPP.

a) Recabar y dar tratamiento lícito a los datos personales, conforme a las disposiciones establecidas en la Ley.[173]
b) Solicitar el consentimiento del titular de los datos personales previo a su tratamiento. (En caso de datos sensibles o patrimoniales, el consentimiento debe ser expreso).[174]
c) No crear bases de datos que contengan datos personales sensibles, sin que se justifique el motivo de su creación y sus finalidades legítimas, concretas y acordes.[175]
d) Procurar que los datos personales contenidos en las bases de datos sean pertinentes, correctos y estén actualizados para los fines para los cuales fueron recabados.[176]
e) Cuando los datos hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad, deberán ser cancelados.[177]
f) Eliminar la información relativa al incumplimiento de obligaciones contractuales una vez que transcurra un plazo de 72 meses, contados a partir de la fecha calendario en la que se presente el incumplimiento.[178]
g) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad. Si se pretende tratar los datos para un fin distinto que no sea compatible o análogo a los fines establecidos, requerirá obtener nuevamente el consentimiento del titular.[179]
h) Realizar esfuerzos razonables para limitar el periodo de tratamiento de los datos personales a efecto de que sea el mínimo indispensable.[180]
i) Tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o los terceros con los que guarde alguna relación jurídica.[181]
j) Comunicar a los titulares la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.[182]
k) Cuando los datos personales no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el cambio en el aviso de privacidad, salvo que el tratamiento sea con fines históricos, estadísticos o científicos.[183]

[173] Artículo 7 de la LFPDPPP.
[174] Artículos 8 y 9 de la LFPDPPP.
[175] Artículo 9 de la LFPDPPP.
[176] Artículo 11 LFPDPPP.
[177] Ídem.
[178] Ibídem.
[179] Artículo 12 de la LFPDPPP.
[180] Artículo 13 de la LFPDPPP.
[181] Artículo 14 de la LFPDPPP.
[182] Artículo 15 LFPDPPP.
[183] Artículo 18 de la LFPDPPP.

l) Establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración y destrucción, o el uso, acceso o tratamiento no autorizado.[184]

m) No adoptar medidas de seguridad menores a las que mantengan para el manejo de su información, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.[185]

n) Informar inmediatamente al titular respecto de las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten, en forma significativa, sus derechos morales o patrimoniales.[186]

o) Guardar confidencialidad respecto de los datos personales a los que den tratamiento, aún después de finalizar sus relaciones con el titular.[187]

En caso de que el INAI tuviera conocimiento, a través del desahogo del procedimiento de protección de derecho o del procedimiento de verificación, sobre algún presunto incumplimiento a las obligaciones que previamente señalamos o a los principios mencionados en el artículo 6 de la Ley, y en los artículos 9 al 19, 23, 36, 40, 44, 45, 47 y 48 del Reglamento de la Ley, se iniciará el procedimiento de imposición de sanciones.

Ahora bien, si el responsable incumple las disposiciones de la Ley o viola alguna de sus obligaciones, para con el correcto tratamiento de los datos personales, también se dará inicio al procedimiento de imposición de sanciones.

En este sentido, es importante destacar que el INAI puede tener conocimiento de este incumplimiento, ya sea a petición de parte, por ejemplo, iniciando un procedimiento de protección de derechos, o en un procedimiento de verificación iniciado ya sea por el propio Instituto o a petición de parte.

El procedimiento de imposición de sanciones inicia con la notificación que el INAI efectúa al presunto infractor de cualquiera de las disposiciones o principios, indicando, de forma clara y pormenorizada, los detalles relativos a los hechos que motivaron la sustanciación del procedimiento. En este sentido, el INAI otorgará un plazo de 15 días al responsable para rendir pruebas y que manifieste por escrito lo que a su derecho convenga. Esto abre la posibilidad para presentar cualquier tipo de pruebas, incluyendo digitales o electrónicas, y desahogarlas. Esto resulta muy conveniente, ya que muchos servicios en

[184] Artículo 19 de la LFPDPPP.
[185] Ídem.
[186] Artículo 20 de la LFPDPPP.
[187] Artículo 21 de la LFPDPPP.

donde se tratan datos personales se encuentran en dispositivos electrónicos o por internet. Ahora bien, en caso de que el responsable no rindiera pruebas, el INAI procederá a resolver con base en los elementos de convicción de que disponga.

El Instituto, tras analizar cada una de las pruebas ofrecidas, así como los demás elementos de convicción que estime procedentes, resolverá de forma definitiva dentro de los 50 días posteriores a la fecha en que inició el procedimiento sancionador en comento. Dicha resolución deberá ser notificada, fehacientemente, a las partes, esto es, tanto al responsable como al particular titular de los datos personales. Dicho plazo podrá ampliarse por el pleno del INAI en una sola ocasión, y por un plazo igual, cuando exista una causa justificada que lo amerite, lo anterior sin que se explique o detalle en alguno de los ordenamientos de la materia que se puede entender por una causa justificada, para que se amplíe el plazo por el pleno del INAI.

En los artículos 140 al 144 del Reglamento de la Ley se establecen las particularidades respecto de la forma, términos y plazos en que se sustanciará el procedimiento de imposición de sanciones, incluyendo reglas para la presentación de pruebas, alegatos, audiencias y cierre de instrucción.

De estos artículos se desprende que el procedimiento de imposición de sanciones tendrá las siguientes etapas:[188]

a) Notificación. Es el aviso inicial que se hace al presunto infractor en su domicilio, va acompañada del informe en donde se detallan los hechos y emplazándolo para que en un término de 15 días contados a partir de que surta efectos la notificación, manifieste lo que a su derecho convenga.
b) Contestación. El presunto infractor manifiesta lo que a su derecho convenga, respecto de todos y cada uno de los hechos que se le imputan en la notificación inicial. Presentará los argumentos por medio de los cuales desvirtúe la infracción que se presume y las pruebas correspondientes. En caso de que las pruebas que se presenten sean periciales o testimoniales, deberán señalarse los nombres y domicilios de los peritos y/o testigos, con el correspondiente interrogatorio o cuestionario respectivamente. Es importante destacar que, si se omite este requisito, las pruebas se tendrán por no ofrecidas.
c) Admisión o desechamiento de pruebas. Una vez ofrecidas las pruebas por el presunto infractor, se dictará un acuerdo de admisión o desechamiento de las mismas para su desahogo correspondiente.

[188] Artículos 140 a 144 del Reglamento de la LFPDPPP.

En ese momento se determina el lugar, fecha y hora para realizar dicho desahogo y se levanta un acta, tanto de la celebración de la audiencia, como del desahogo de las pruebas admitidas.

d) Cierre de instrucción y resolución. Una vez que se han desahogado las pruebas que fueron admitidas, se notificará al presunto infractor para que en un término de cinco días contados a partir del día siguiente al que surta efectos la notificación, pueda presentar los alegatos que considere pertinentes. Al término de este plazo, se cerrará la instrucción y el INAI deberá emitir su resolución en un plazo no mayor a los 50 días siguientes de que dio inicio el procedimiento.

Una vez resuelto el procedimiento de imposición de sanciones, en el caso de existir alguna inconformidad, se puede presentar en contra de la resolución un juicio de nulidad ante el ahora Tribunal Federal de Justicia Administrativa.

Conclusiones

Como podemos apreciar del desarrollo del presente apartado, el procedimiento de imposición de sanciones es producto de una acentuada y cuidadosa verificación que la misma ley ordena al órgano garante para comprobar que el responsable de datos personales ha infringido alguna disposición normativa contemplada en la ley. Una vez observadas las irregularidades, omisiones u actos constitutivos de las faltas contempladas en el ordenamiento jurídico, es entonces cuando se tiene la posibilidad de iniciar el mencionado procedimiento.

Referencias

García, E. (1998). *Introducción al Estudio del Derecho*. México. Porrúa.

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

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

INAI. Resoluciones. Consultado en: *http://inicio.ifai.org.mx/SitePages/ResolucionesPDP.aspx*

DOF. (2015). *Acuerdo mediante el cual se aprueban los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones*. México.

INAI. (2011). *Guía práctica para la atención de las solicitudes de ejercicios de los derechos ARCO*. México.

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).

CAPÍTULO X
DE LAS INFRACCIONES Y SANCIONES

CAPÍTULO X
DE LAS INFRACCIONES Y SANCIONES

Artículo 63. *Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:*

I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley.

II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales.

III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable.

IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley.

V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley.

VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares.

VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64.

VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley.

IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12.

X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos.

XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.

XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley.

XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible.

XIV. Obstruir los actos de verificación de la autoridad.

XV. Recabar datos en forma engañosa y fraudulenta.

XVI. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares.

XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley, y XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.

Artículo 64. *Las infracciones a la presente Ley serán sancionadas por el Instituto con:*

I. El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en la fracción I del artículo anterior.

II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior.

III. Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior.

IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Artículo 65. *El Instituto fundará y motivará sus resoluciones, considerando:*

I. La naturaleza del dato.

II. La notoria improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular, en términos de esta Ley.
III. El carácter intencional o no, de la acción u omisión constitutiva de la infracción.
IV. La capacidad económica del responsable.
V. La reincidencia.

Artículo 66. *Las sanciones que se señalan en este Capítulo se impondrán sin perjuicio de la responsabilidad civil o penal que resulte.*

COMENTARIO

Nuhad Ponce Kuri

Introducción

Sin lugar a dudas, uno de los desafíos de la ley que en comento es el establecimiento de infracciones y sanciones. Como sabemos, el debido cumplimiento de esta ley no sólo se agota a partir del establecimiento de un simple aviso de privacidad o del mero compromiso ético de cumplirla, por el contrario, es necesario el establecimiento de mecanismos organizacionales que permitan respaldar el trabajo que se hace en materia de protección de datos en manos de los llamados responsables por el ordenamiento jurídico.

La ley de datos estaría incompleta sin este catálogo de infracciones y sanciones que se vuelve medular para impedir el incumplimiento. Sabemos que para el maestro García Máynez las normas pueden clasificarse desde su sanción en:

- Leyes *perfectae*: aquellas que, en caso de violarse, su sanción consiste en la nulidad o inexistencia del acto que las vulnera.
- Leyes *pluscuamperfectae*: son las que imponen al infractor un castigo, además de una sanción pecuniaria.
- Leyes *minus cuam perfectae*: son las que al no poder impedir que el acto violatorio produzca efectos jurídicos, establecen una sanción o pena a la persona que comete la violación de la norma.
- Leyes *imperfectae*: aquellas que no tienen una sanción.[189]

El incumplimiento a las disposiciones de esta Ley dan origen a un apercibimiento, el pago de multas, y en su caso, penas privativas de libertad,

[189] García, E. (1998). *Introducción al Estudio del Derecho*. México. Porrúa, p. 89.

pero no pueden nulificar o hacer inexistente la violación, por lo que podemos decir que nos encontramos frente a una norma *minus cuam perfectae*.

El capítulo que comentamos es la concreción material de la Ley en acciones determinadas y, sobre todo, orientada a los casos en los cuales el incumplimiento implica un castigo para el responsable. Para realizar esta tarea, hemos decidido hacer un análisis del contenido global, pero que revise todas y cada una de las infracciones que propone la Ley. En ese sentido, hemos encasillado conceptualmente las infracciones para desarrollarlas en un conjunto temático que abarque algunas de ellas y, al finalizar cada apartado, el lector encontrará un par de casos que le permitirán entender el impacto de las mismas en la concreción organizativa del responsable.

Correlaciones

Del artículo 140 al 144 de la Ley Federal de Protección de Datos en Posesión de los Particulares.

Análisis de contenido

En su artículo 63, la Ley establece un listado de todos los supuestos de infracción en los que el responsable será sancionado en caso de actualizarse alguna de las hipótesis señaladas. En estas 19 infracciones se contemplan conductas de dar, hacer y de no hacer por parte del responsable. Curiosamente, la última habla sobre el incumplimiento del responsable a cualquiera de las obligaciones establecidas a su cargo por la Ley, ello podría representar un error de técnica legislativa pues nos conduciría a preguntarnos sobre la necesidad de enlistar las dieciocho conductas previas. En realidad, el legislador contempló el listado en virtud de que, para la imposición de sanciones, se realizó una segmentación de las dieciocho conductas en dos grandes rubros para tasar la pena aplicable:

a) de 100 a 160 mil días de salario mínimo vigente en la Ciudad de México: en los casos mencionados en las fracciones II a VII del artículo 63 y
b) de 200 a 320 mil días de salario mínimo vigente en la Ciudad de México: en los casos mencionados en las fracciones VIII a XVIII del mismo artículo.

Aunado a lo anterior, en caso de reincidencia o persistencia en la comisión de infracciones, se establece una sanción adicional de 100 a 320 mil días de salario mínimo vigente en la Ciudad de México, y en caso de tratarse de datos sensibles, las sanciones podrán incrementarse hasta al doble.

Solicitudes

Entrando en materia, encontramos las tres primeras fracciones referidas al tratamiento de las solicitudes de derechos ARCO. La primera conducta prevista por la Ley es la referida a la falta del cumplimiento con la solicitud al titular del derecho. En este caso el responsable tiene la obligación de dar tratamiento a cualquier solicitud de ejercicio de los derechos ARCO que reciba, en términos de lo que señalan los artículos 28 al 35 de la Ley y 87 al 100 del Reglamento. Por lo que la sanción prevista en esta fracción puede generarse por el incumplimiento del responsable a cualquiera de las disposiciones antes señaladas.

Algunos ejemplos comunes de incumplimiento a las obligaciones que prevé esta fracción son:

1. No dar respuesta o hacer efectiva la solicitud en los plazos fijados por el artículo 32 de la Ley.
2. Hacer caso omiso de la solicitud o no dar respuesta alguna.
3. No cerciorarse de la identidad del titular, en términos de lo señalado por la guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO.[190]

En ese sentido, es de medular importancia que los responsables trabajen dentro de sus políticas, procedimientos y manuales de atención a derechos ARCO para dar puntual atención al momento de recibirlas y capacitar al comité de privacidad o a la persona designada para que pueda cumplir con el ejercicio de las solicitudes. Es imperante para los responsables llevarlo a cabo, pues de lo contrario nos encontramos con la falta de garantía de los derechos ARCO al seno de la organización responsable.

De igual manera ocurre con el tratamiento de la solicitud, pues el actuar con negligencia o dolo en la tramitación de la misma constituye un efecto nocivo que acarrea un castigo. En este supuesto nos referimos a engañar al titular de datos personales al momento de dar respuesta a una solicitud, esto es, que para actualizarse este supuesto, forzosamente debe haber una respuesta por del responsable. Puede ser que la respuesta argumente, por ejemplo, que no es posible atenderla en virtud de alguna causa que no es justificada por la Ley o responderla de manera inadecuada, ya sea por negligencia, dolo o por algún interés particular del responsable.

El dolo o la negligencia contemplada en la Ley nos conduce a poner al responsable en una situación de cuidado con respecto al tratamiento de los

[190] INAI. (2011). *Guía práctica para la atención de las solicitudes de ejercicios de los derechos ARCO*, p. 7.

datos personales. En ese sentido, entenderemos que el dolo se actualizará en la respuesta a la solicitud que oculte o niegue la información a sabiendas de que se encuentra en manos del responsable. Por su parte, la negligencia la situaremos en el extremo de la falta de cuidado al responder y se actualiza cuando encontramos en la organización descuido en la implementación de políticas o procedimientos para atender debidamente las solicitudes.

Aunque se piense lo contrario esto es muy común en la práctica. Una respuesta frecuente de algunos responsables es argumentar la inexistencia de los datos, siendo que sí están en su poder. Esto se ha visto, ya sea por no tener una base de datos ordenada, o por querer continuar con el tratamiento de los datos, a pesar de que titular ejerza sus derechos ARCO.

Sirva para ilustrar lo anterior el siguiente caso solventado por el Instituto.

> Responsable: El nombre no está disponible.
>
> Con fecha 15 de diciembre 2015, el Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales recibió la denuncia de un titular en la cual explicaba que un responsable le había negado la solicitud de ejercicio de derechos de acceso, oposición y cancelación que intentó presentarle por escrito. Por lo que, con el fin de que las llamadas cesaran realizó la denuncia. Debido a esta infracción, el responsable fue sancionado con el apercibimiento de hacer efectiva la solicitud de ejercicio de derechos ARCO del denunciante y con una multa de 42 mil sesenta pesos, por no dar respuesta a la solicitud de ejercicio de derechos ARCO del denunciante.[191]

Principios

Uno de los objetivos de la Ley es el cabal cumplimiento de los principios que orientan el tratamiento de datos personales. En ese sentido, es de llamar la atención que la Ley le otorga un carácter de fuerza a dichos principios y no sólo los considera enunciativos sino que su falta de cumplimiento conllevan una sanción. Así el artículo 6 de la Ley señala los principios rectores bajo los que se debe dar tratamiento a los datos personales. Dice la ley que:

> Artículo 6. Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley.

[191] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0037/16.

El incumplimiento de cualquiera de los principios generará una sanción. Es importante tomar en cuenta lo señalado por el reglamento de la Ley. La casuística en este sentido es variada. A continuación, la ilustramos con algunos casos que el Instituto ha solventado.

> Responsable: World Travel Servicios Turísticos, S.A. de C.V.
>
> Con fecha 12 de marzo 2015, el entonces Instituto Federal de Acceso a la Información, actualmente Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales recibió la denuncia de un titular en la cual explicaba que recibió una invitación telefónica para acudir a un restaurante y recoger un premio consistente en un viaje de tres días y dos noches a un destino turístico, lo anterior, por ser muy buen cliente del banco.
>
> Únicamente le pidieron que llevara su tarjeta, la señora dijo que asistió al restaurante para renunciar al premio, alegando problemas de salud. Sin embargo, alegó haberse levantado al sanitario y dejar sus tarjetas en la mesa. Al regresar, la persona que la atendió le dijo que debía firmar la "renuncia de su premio". La señora dijo que necesitaba sus lentes, pero de igual forma firmó. Al llegar a su casa se dio cuenta de que había firmado una transferencia bancaria por 28 mil 500 pesos, llamó al banco, pero le negaron ayuda.
>
> Debido a estas infracciones, World Travel Servicios Turísticos, S.A. de C.V. fue sancionada **por contravenir los principios de información, responsabilidad y licitud con una multa** de 280 mil 400 pesos. También fue multada con 385 mil 550 pesos por omisiones en su aviso de privacidad. Por último fue multada con 420 mil 600 pesos por **no responder a la solicitud de información realizada por el Instituto**. Dando un total de 1millón 402 mil pesos.[192]

El caso narrado anteriormente se sitúa en los diversos supuestos que hemos trabajado, pues el responsable es sancionado por contravenir los principios de información vinculados al aviso de privacidad, que debe darse a conocer previo al tratamiento de los datos, al principio de responsabilidad, pues claramente se hizo un tratamiento desprolijo de los datos personales del titular del derecho y del principio de licitud al no cumplir de manera adecuada con el ordenamiento jurídico en materia de datos personales.

Veamos otro caso relevante que puede ilustrar la falta de cumplimiento de los principios:

[192] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0034/16.

> Responsable: El nombre no está disponible.
>
> Con fecha 23 de junio 2015, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de Datos recibió la denuncia de un titular en la cual explicaba que solicitó copia de su expediente médico a su "doctor", quien le respondió que por tratarse de "manejo de datos personales" únicamente le podía proporcionar un informe médico. La titular ingresó al sitio web de la clínica privada del doctor, para solicitar su información por medio del aviso de privacidad. Sin embargo, dicho aviso de privacidad no aparecía en la página web. Debido a estas infracciones, "el doctor" fue sancionado con una multa de 6 mil 476 pesos **por incumplir los principios de información, responsabilidad y licitud**. De igual manera fue sancionado con una cantidad igual, **por omitir poner a disposición el aviso de privacidad**. Asimismo, al **recabar y tratar datos personales sensibles, sin consentimiento expreso del denunciante y por escrito**, se le impuso una multa de 12 mil 952 pesos; la cual se incrementó 50 por ciento por tratarse de datos personales sensibles a 6 mil 476 pesos. Por último, fue sancionado con 14 mil veinte pesos por **obstruir el procedimiento de verificación del Instituto.** Dando un total de 46 mil 400 pesos.[193] (Énfasis añadido).

Como podemos observar, este caso adquiere fuerza justamente en el incumplimiento de los principios de información, responsabilidad y licitud. Claramente la falta de cumplimiento de las disposiciones normativas en materia de aviso de privacidad, políticas y procedimientos nos conduce a este tipo de infracciones vinculadas con la falta de cumplimiento de los principios orientadores en materia de protección de datos.

Elementos del aviso de privacidad y cambio de finalidades del mismo

A la par de lo anterior, es claro que la ley contemple una infracción y sanción especial vinculada a la carencia u omisión de alguno o de todos los elementos que lo conforman.

El principio de información está colmado en el documento en físico o electrónico que se pone a disposición del titular previo al tratamiento de los datos. En ese sentido, el no referir quién es el responsable o dónde se encuentra su domicilio, las finalidades para las que se tratan los datos, las transferencias que se efectúan o los procedimientos para hacer efectivos los derechos ARCO constituirán infracciones y sanciones por parte de la ley. Veamos un caso que nos permita ilustrar lo anterior.

[193] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0002/16.

> Responsable: Instituto Internacional Libertad, A.C.
>
> Con fecha 6 de mayo de 2014, el entonces Instituto Federal de Acceso a la Información, actualmente Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales recibió la denuncia de un titular, en la cual una persona explicaba que una de sus hijas menores le comentó que aparecía una foto de ella en Google. El padre de las menores buscó en Google, y encontró fotos de sus hijas en el sitio *web* de la escuela, haciendo referencia a que ambas estaban becadas, su nombre y grado escolar. El señor alegó que jamás dio su consentimiento, ni firmó ningún aviso de privacidad con **la escuela**. Debido a estas infracciones, el Instituto Internacional Libertad, A.C. fue multado con 67 mil 290 pesos por contravenir los principios de licitud, consentimiento, información y responsabilidad. También fue multada con 140 mil 097 pesos **por darle un tratamiento distinto al previsto en su aviso de privacidad.** Por último, fue sancionada con $200 mil 053 pesos por **obstruir el procedimiento de verificación del Instituto**. Dando un total de 407 mil 440 pesos.[194] (Énfasis anadido).

Aún y cuando este caso trae aparejadas otras sanciones, es imperante detenernos en la que establece que hubo un tratamiento distinto al previsto en el aviso de privacidad. En este caso actualizamos que, habiendo el documento, el tratamiento no cumple con las finalidades del mismo por lo que podemos interpretar que una de las partes del aviso no se actualiza. Las finalidades del tratamiento deben estar contempladas de la manera en la que se lleva a cabo dicho tratamiento, pues de lo contrario produce los efectos de finalidades no previstas en el aviso de privacidad.

En ese sentido reafirmamos que si se omite alguno de estos requisitos, el responsable será acreedor a una sanción, independientemente de la que se le pueda imponer por alguna verificación o algún otro incumplimiento. Veamos otro caso.

> Responsable: Servicios Profesionales IMEX, S.A. de C.V**.**
>
> Con fecha 14 de noviembre 2014, el entonces Instituto Federal de Acceso a la Información, actualmente Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales recibió la denuncia de un titular en la cual explicaba que fue dado de alta en el IMSS y dado de baja el mismo día de su "alta" por una persona moral con la cual no tenía ninguna relación laboral. Debido a estas infracciones, Servicios Profesionales IMEX, S.A. de C.V. fue sancionada con una multa de 269 mil 160 pesos por incumplir los principios de **información, responsabilidad y licitud**. De

[194] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0005/15.

> igual manera fue sancionado con 134 mil 580 pesos, **por omisiones en su aviso de privacidad**. Finalmente fue multada con 403 mil 740 pesos por **transferir datos patrimoniales** a terceros. Dando un total de 807mil 480 pesos.[195] (Énfasis anadido).

Como podemos observar una de las sanciones deviene de las omisiones del aviso de privacidad, pues el titular del derecho nunca recibió la información adecuada y pertinente respecto a lo que ocurriría con su tratamiento de datos.

La misma Ley contempla como infracción que trae aparejada una sanción, el cambio de finalidades para las cuales fueron otorgados los datos. En ese sentido el principio de lealtad refiere que el consentimiento va relacionado íntimamente con las finalidades. Esto es que se debe solicitar al titular el consentimiento para el uso de sus datos personales en estricto apego a las finalidades para los cuales fueron recabadas. En caso de variar o cambiar se debe solicitar otro consentimiento, honrando aquel principio.

Datos inexactos o no cancelados

Al igual que sucede con la carencia de las partes del aviso de privacidad es imperante referir que el mantener datos inexactos o bien no cancelarlos cuando se solicitan constituye —de igual manera— una infracción que merece ser sancionada. En ese sentido baste recordar que dar información inexacta incumple con el principio de calidad de la información, por lo que la carencia de procedimientos que permitan la actualización constante de las bases de datos o la falta de procedimientos para que el titular pueda llevar a cabo la rectificación de sus datos serán situaciones sancionables.

De manera más radical encontramos la carencia de cancelación de los datos. Sabemos que esto conduce al responsable a la acumulación de ellos que le han pedido cancelar y por consiguiente abre una brecha de seguridad en el tratamiento de datos.

El procedimiento ordenará que una vez que se solicite la cancelación, deberá colocar los datos en una lista de bloqueo y posteriormente proceder a la cancelación. Si no existen políticas y procedimientos de cancelación al seno de las organizaciones ocurrirá una posible sanción. Observemos los siguientes dos casos:

> Responsable: Impulse Telecommunications de México, S.A. de C.V.

[195] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0041/15.

> Con fecha 23 de junio 2014, el entonces Instituto Federal de Acceso a la Información, actualmente Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales recibió la denuncia de un titular en la cual explicaba que recibió múltiples llamadas de una compañía de seguros, referente a una póliza que nunca contrató. Toda vez que nunca otorgó sus datos personales. Por lo que, con el fin de que las llamadas cesaran, realizó la denuncia. Debido a estas infracciones, "Impulse Telecommunications de México, S.A. de C.V." fue sancionada con 403 mil 740 pesos por incumplir los principios de información, responsabilidad y licitud. De igual manera fue sancionada con una multa de 538 mil 320 pesos, **por mantener datos personales inexactos en su base de datos.** Dando un total de 942 mil 020 pesos. (Énfasis anadido).
>
> Responsable: 2Access, S.A. de C.V.
>
> Con fecha 19 de marzo 2015, el entonces Instituto Federal de Acceso a la Información recibió la denuncia de un titular en la cual explicaba que empezó a recibir cargos en su estado de cuenta por parte de esta empresa. Él desconocía todos los cargos y negaba tener vínculo alguno con dicha empresa, la **empresa comprobó arrendar la base de datos de un tercero**. Sin embargo, **negó contar con** los **datos del denunciante.** Debido a esta infracción, 2Access, S.A. de C.V. fue sancionado con una multa de 15 mil 71 pesos y cincuenta centavos.[196] (Énfasis anadido).

Deber de confidencialidad

Este es un deber expreso de confidencialidad para el tratamiento de datos personales, por ende, su incumplimiento es considerado una infracción que amerita una sanción. Al hablar de responsable o terceros, se extiende esta obligación al encargado, los empleados, funcionarios, comisionistas y/o profesionistas a cargo del responsable, o algún tercero que, por alguna relación jurídica, dé tratamiento a los datos personales del titular.

Como sabemos, la confidencialidad es un deber inherente al resguardo de la vida privada de las personas y así se encuentra contemplado en nuestro marco constitucional en su artículo 16. La autodeterminación informativa no es una excepción y guarda el mismo deber que el resto de los ámbitos de la vida privada. En ese sentido, todos aquellos que participan en el tratamiento de datos se encuentran obligados a mantener a salvo dicho deber. Veamos el siguiente caso que resuelve el Instituto.

[196] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0005/16.

> Responsable: Radiomóvil Dipsa, S.A. de C.V. (Telcel).
>
> Con fecha 16 de abril 2013, el Instituto Federal de Acceso a la Información y Protección de Datos recibió una denuncia de un titular, en la cual explicaba que celebró un contrato con Telcel, el cual venció por falta de pago, lo que conllevó a que el departamento de cobranza empezara a comunicarse con los conocidos del titular para exigir el pago del cumplimiento del contrato. Posteriormente, esta información fue comprobada por el gerente del departamento de cobranza, al confirmar que se empezaron a comunicar con los conocidos del titular, debido a la falta de respuesta del mismo. Por estas infracciones, Radiomóvil Dipsa, S.A. de C.V. (Telcel) fue sancionado con una multa de 1 millón 813 mil 280 pesos. De igual manera fue sancionado con una multa de 1 millón 813 mil 280 pesos **por incumplir el deber de confidencialidad establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.** Así mismo con otra multa de 3 millones 108 mil 480 pesos por vulnerar la seguridad de bases de datos locales, programas o equipos y finalmente, con una multa de 1 millón 942 mil 800 pesos por recabar o transferir datos personales sin el consentimiento expreso del titular.[197] (Énfasis anadido).

Veamos otro caso similar que violenta el deber de confidencialidad.

> Responsable: El nombre no está disponible**.**
>
> Con fecha 17 de febrero 2015, el entonces Instituto Federal de Acceso a la Información, actualmente Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales recibió la denuncia de un titular, en la cual explicaba que recibió múltiples llamadas a todas las extensiones telefónicas de su trabajo, por medio de las cuales se le requería un presunto pago. Las llamadas no sólo eran dirigidas a ella, sino a compañeros de trabajo en las que les decían que convencieran al denunciante de realizar el pago, dejar de ser moroso y de "hacerse sonso". El denunciante remarcó el número telefónico y descubrió que correspondía a un despacho de cobranza. Debido a estas infracciones, "el despacho de cobranza" fue sancionado con una multa de 7 mil 10 pesos por **contravenir** con los principios de lealtad, responsabilidad y licitud. De igual manera, fue sancionado con una multa de 14 mil veinte pesos **por incumplir con el deber de confidencialidad**. Así mismo, se le impuso una multa de 114 mil veinte pesos **por** tratar datos personales del denunciante para una finalidad distinta a la original**.** También recibió una multa por 14 mil veinte pesos, debido a que **transfirió datos personales de carácter patrimonial del denunciante sin**

[197] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, Procedimiento de Imposición de Sanciones. Expediente: PS.0026/13.

> **su consentimiento** expreso. Por último, fue sancionado con 14 mil veinte pesos por obstruir el proceso de verificación del INAI. Dando un total de 63 mil noventa pesos.[198] (Énfasis anadido).

Como podemos apreciar en los casos expuestos, una práctica recurrente de los servicios de cobranza es justamente llamar a los conocidos o referencias que el titular proporcionó para la celebración del contrato. El Instituto entendió que esas llamadas atentaban contra el deber de confidencialidad al proporcionar información sobre el titular. Es imperante que tanto en las políticas como en los procedimientos los responsables cuenten con convenios expresos de confidencialidad que refieran esta obligación específicamente y de manera expresa, aunque este deber se traduce en acciones concretas más allá de que sean o no dichos convenios entre diversas partes del tratamiento, pues el deber es inherente al titular.

Transferencias

Sin lugar a dudas, uno de los temas más delicados del tratamiento de datos es el apartado de transferencias. Por tal motivo la Ley prevé tres fracciones del apartado de infracciones en las transferencias. Estos tres supuestos diversos son considerados infracciones:

a) Transferencias sin acompañamiento del aviso de privacidad.
b) Transferencias no permitidas por la ley.
c) Transferir datos sin el consentimiento del titular.

Como podemos apreciar, el tratamiento de datos personales incluye la divulgación de los mismos, la cual debe entenderse, no de manera libre o sin límites, sino sujeta a limitaciones y, fundamentalmente, al consentimiento del titular del derecho. Así, sabemos que toda transferencia de datos obliga al responsable a comunicar el aviso de privacidad al receptor, el cual deberá avisar los cambios de finalidades en el primer contacto que tenga con el titular del derecho en un nuevo aviso de privacidad. En ese sentido, la Ley sanciona no contemplar el mecanismo de acompañamiento del aviso de privacidad.

Al igual que sucede en el supuesto anterior, encontramos otro que está vinculado con el consentimiento de las transferencias. Así, debemos entender que toda transferencia debe encontrarse consentida por el titular del derecho y ello abre algunas interrogantes: ¿Basta el consentimiento tácito? y, ¿es necesario el consentimiento expreso? La ley precisa, en su artículo 36, que toda transferencia deberá venir acompañada del consentimiento expreso. Sin embargo, existen algunas transferencias que los responsables llevan a

[198] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0043/15.

cabo por mandato de ley, en las cuales encontramos que no es necesario el consentimiento del titular, ni que el responsable establezca medidas adicionales para la obtención del consentimiento. En virtud de ello y respecto a las condiciones del consentimiento en transferencias, podemos decir que, tratándose de transferencias primarias derivadas de la ley y sin las cuales dicho acto o relación jurídica no podría perfeccionarse en su totalidad, debemos entender que no es necesario que medie el consentimiento. Por el contrario, en el caso de otro tipo de transferencias que podemos llamar secundarias, es necesario establecer las condiciones necesarias para recabar el consentimiento expreso, el cual será objeto de revisión por parte del Instituto.

Traigamos a colación el último caso expuesto anteriormente cuando hablamos del deber de confidencialidad que ilustra también la indebida transferencia de datos de carácter patrimonial. Utilizaremos el caso transcrito un par de páginas atrás por lo que sólo citaremos la parte conducente

> Responsable: El nombre no está disponible.
>
> "….. Asimismo, se le impuso una multa de 14 mil veinte pesos por tratar datos personales del denunciante para una finalidad distinta a la original**.** También recibió una multa por 14 mil veinte pesos, debido a que **transfirió datos personales de carácter patrimonial del denunciante sin su consentimiento** expreso. Por último, fue sancionado con 14 mil veinte pesos por obstruir el proceso de verificación del INAI. Dando un total de 63 mil noventa pesos.[199]

Como podemos observar, en este caso existe la conducta de transferencia de datos personales de carácter patrimonial sin que exista previamente el consentimiento expreso del titular y tiene como consecuencia la sanción del Instituto. En ese sentido, recalcamos la imperiosa necesidad de contemplar, para el caso de transferencias, el mecanismo adecuado para la obtención del consentimiento expreso por parte del titular del derecho.

Medidas de seguridad

Cuando se habla de vulneraciones a la seguridad de los datos personales, normalmente se piensa en un *hacker* o alguien externo con un interés malicioso de tener acceso a un dispositivo, ordenador o una base de datos sin autorización. Sin embargo, las vulneraciones de seguridad se dan, en su mayoría, por personas al interior de la propia organización, es decir no necesariamente involucran un *hacker*, entendiéndolo como alguien ajeno y externo. Estas vulneraciones se pueden dar en cualquiera de los tres niveles de

[199] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0043/15

las medidas de seguridad. En el ámbito físico pueden ocurrir, por ejemplo, en los formatos físicos en donde se recaban datos o en las instalaciones mismas que soportan los datos recabados por la organización. En el plano técnico, se encontrarán vinculadas a los procesos de cuidado del almacenamiento de los datos en soportes digitales. En ese sentido, la falta de cuidado de los equipos de remoción móvil como computadoras portátiles, dispositivos de telefonía móvil o tabletas electrónicas donde se respalda información, constituyen una vulneración a la seguridad. El tercer nivel son las medidas de seguridad administrativas en donde la formación de políticas y procedimientos en el seno de la organización constituyen un eje motor de su cuidado.

Las vulneraciones a las que se refiere la Ley señalan una imputabilidad directa del responsable. Este supuesto puede actualizarse si no cumpliera con el principio de responsabilidad señalado en el artículo 19 de la Ley. Esto es, que no se tengan, no sean suficientes o no se haya cumplido con las medidas de seguridad físicas, técnicas y/o administrativas para proteger los datos personales que recaba el responsable. Es por ello que debe contemplar auditorías de revisión de las medidas de seguridad físicas, técnicas y administrativas, por lo menos una vez al año y llevar una bitácora de su implementación.

Obstrucción de actos de autoridad

El INAI tiene facultades para verificar el cumplimiento de la Ley, su reglamento, lineamientos y demás ordenamientos vigentes en materia de protección de datos personales.[200] Durante esta verificación, el Instituto puede requerir acceso a la información y/o documentación que considere necesaria o importante para poder emitir una resolución. El no permitir y/o colaborar con la presentación o facilitación de la documentación o información genera la imposición de una sanción, en los términos de lo señalado por esta fracción.

Veamos un par de casos resueltos por el Instituto que nos permiten ilustrar lo previsto en la Ley como obstrucción de los actos de verificación del Instituto.

> Responsable: Colegio Panamericano de Texcoco, A.C.
>
> Con fecha 3 de septiembre 2015, el entonces Instituto Federal de Acceso a la Información, actualmente Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales recibió la denuncia de un titular, en la cual explicaba que recibió múltiples llamadas de diversas personas que se identificaron como parte del personal de la escuela de sus hijas. Las cuales le detallaron entre burlas y amenazas. La denunciante no

[200] Artículos 59 y 60 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

había firmado ningún aviso de privacidad y sus datos los proporcionó al llenar la solicitud de inscripción a la escuela. Debido a estas infracciones, "Colegio Panamericano de Texcoco, A.C." fue sancionado con una multa de 70 mil 100 pesos por incumplir con los principios de consentimiento, información, responsabilidad y licitud. De igual manera fue sancionado con una multa de 49 mil 981 pesos con 30 centavos por incumplir con los elementos relativos al aviso de privacidad. **Así mismo, fue multado con 99 mil 962 pesos con 60 centavos por obstruir el procedimiento de verificación del INAI**. Dando un total de 220 mil 43 pesos con 90 centavos.[201] (Énfasis anadido).

Responsable: Operadora Oceánica Internacional, S.A. de C.V.

El pleno del Instituto impuso una multa de 2 millones 493 mil 200 pesos a Operadora Oceánica Internacional, S.A. de C.V. por violar la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). La sanción fue acordada por unanimidad en el órgano colegiado después de que se acreditó que la empresa no pudo desvirtuar el haber obstruido actos de verificación ordenados por el INAI.

El procedimiento fue ordenado a partir de que el Instituto tuvo conocimiento de que en una nota periodística del 18 de mayo de 2011 se hicieron públicos los datos de una persona "que presuntamente" había sido paciente del "Centro de rehabilitación Oceánica". En dos ocasiones (23/05/11 y 12/07/11), **el INAI solicitó** a la **empresa un informe** relacionado con dicha publicación **pero no atendió ninguno de ellos.** Ante la negativa, el Instituto ordenó una visita de verificación a Operadora Oceánica Internacional, S.A. de C.V. en sus instalaciones en Mazatlán Sinaloa; sin embargo, cuando el personal comisionado se presentó al domicilio, no se le dieron las facilidades correspondientes y se le negó el acceso al inmueble**, obstruyendo con ello los actos de verificación de la autoridad.**

En razón de lo anterior, el Pleno del Instituto determinó el 21 de marzo de 2012 el inicio de un procedimiento de imposición de sanciones. Inconforme con esta resolución, la empresa presentó un juicio de nulidad ante el entonces Tribunal Federal de Justicia Fiscal y Administrativa, autoridad que el 8 de abril de 2013 dictó sentencia definitiva en contra de Oceánica. Con este fallo, se dio continuidad al procedimiento en contra de Operadora Oceánica Internacional, S.A. de C.V., el cual quedó resuelto con la imposición de la citada multa por la obstrucción del procedimiento de verificación previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Donde dicha ley establece que constituyen infracciones a la misma, "obstruir los actos de verificación de la autoridad".[202] (Énfasis anadido).

[201] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0023/16.

[202] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0001/12.

Como podemos observar, en ambos casos encontramos la conducta infractora a la Ley. Es imperante recordar que el procedimiento de verificación permite al Instituto verificar el cumplimiento normativo en el lugar donde se lleva, preponderantemente, el tratamiento de los datos. El procedimiento de verificación deriva justamente del incumplimiento de una resolución dictada por el Instituto sobre un procedimiento de protección de datos personales o bien de la denuncia que se lleva a cabo al pleno del Instituto y que, dependiendo de diversos factores, puede ordenar la verificación. El signo común es la presunción de incumplimiento de los principios orientadores en materia de datos. Es por ello que dentro de las políticas y procedimientos que se construyen en el seno de la organización, se deberá contemplar el de atender, en todo momento, las visitas de la autoridad.

Tratamiento de datos (captación, uso y almacenamiento)

De la fracción XV a la fracción XVIII del artículo encontramos un conjunto de infracciones relativas al uso de los datos. Ahí están contenidas diversas fases del tratamiento en donde se puede sancionar al responsable. Así, recabar los datos de forma engañosa o fraudulenta impacta directamente en el principio de licitud, el cual no sólo derivará en una infracción pecuniaria, sino —como se verá en el capítulo relativo a tipos penales— se considera un delito en la materia. A la par encontramos una infracción derivada del derecho de cancelación, en donde la conducta infractora versará sobre el uso ilegítimo de los datos, aún y cuando se lleve a cabo el derecho de cancelación. En este último supuesto, la autoridad deberá verificar que los datos efectivamente se siguen utilizando y que prevalecen las medidas de seguridad respecto las listas de bloqueo que se originan inmediatamente se pide la cancelación.

Otro supuesto de infracción tiene que ver con un tratamiento de los datos vinculados a generar el impedimento del ejercicio de los derechos ARCO. Este supuesto normativo se encuentra orientado a los casos en donde la falta de prolijidad en el uso impide dar acceso a la información, aún y cuando se tenga la certeza de que se entregó el dato, o bien que imposibilite al titular del derecho a generar la rectificación de los mismos. De igual manera sucede cuando el responsable no genera mecanismos de oposición para finalidades secundarias o no incorpora en el aviso de privacidad el mecanismo de negativa de tratamiento. En todos ellos el responsable se hará acreedor de una sanción.

Otra infracción que ha generado diversas sanciones es la creación de bases de datos sensibles sin justificación y sin perseguir finalidades legítimas y concretas orientadas por la actividad propia del responsable. En ese sentido y, tratándose de datos sensibles, el responsable deberá, en todo momento, si trata datos sensibles, encontrar plena justificación de ello, incorporarlo a su

aviso de privacidad y contemplar las medidas de seguridad oportunas para su protección. Veamos algunos casos relevantes:

> Responsable: Sport City, S.A. de C.V.
>
> El 6 de junio de 2012, el Instituto Federal de Acceso a la Información y Protección de Datos recibió una denuncia por presuntas violaciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) donde se mencionaba que **Sport City, S.A. de C.V.** en su aviso de privacidad en la página de internet omitia **que los titulares de los datos personales podían oponerse al tratamiento de los datos personales**, lo que implicó que se iniciara un proceso de verificación en su contra, y al ser correcta la información, se procediera a un procedimiento de imposición de sanciones. El Instituto Federal de Acceso a la Información y Protección de Datos Personales impuso una multa de 1 millón 246 mil 600 pesos por omitir en el aviso de privacidad alguno o todos los elementos que este debe contener.[203] (Énfasis anadido).
>
> Responsable: Banco Mercantil del Norte, S.A., Institución de Banca Múltiple, Grupo Financiero Banorte.
>
> El 22 de enero de dos mil catorce, el entonces Instituto Federal de Acceso a la Información y Protección de Datos, actualmente Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales recibió una denuncia de una titular en contra de Banco Mercantil del Norte, S.A., Institución de Banca Múltiple, Grupo Financiero Banorte por presuntas violaciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, señalando que un contrato que celebró de crédito automotriz denominado "Auto-estrene de Banorte" nunca se incluyó algún aviso de privacidad y de que de igual manera nunca otorgo su consentimiento para el tratamiento de sus datos personales, **sin embargo, sus datos personales fueron transmitidos a un tercero llamado "**Integra Capital**", quien debido a esto, vulneró su integridad.**
> Posteriormente al analizar la situación, el INAI inició un procedimiento de verificación que resultaría a favor de la titular de los datos personales, para posteriormente iniciar el procedimiento de sanciones en contra de los grupos mencionados previamente, quienes fueron sancionados con una multa aproximada de 18 millones 544 mil 200 pesos **debido a que recabaron datos personales sensibles sin su consentimiento.** De igual manera fueron sancionados con otra multa aproximadamente de 18 millones 544 mil 200 pesos. Debido a que se encontraron datos de la persona (sin su consentimiento) recabados en su base de datos y por último se le impuso

[203] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, Procedimiento de Imposición de Sanciones. Expediente: PS.0004/12.

> una multa de 18 millones 544 mil 200 pesos, debido a que los grupos mencionados anteriormente no pusieron a disposición del titular un aviso de privacidad.[204] (Énfasis anadido).

Sanciones

Por lo que respecta a las multas, la Ley las cuantifica tomando como base el salario mínimo vigente en la CDMX. Sin embargo, al día de hoy, y con base en el decreto publicado en el *Diario Oficial de la Federación* el día 27 de enero de 2016, de acuerdo con la reforma constitucional del artículo 26 Apartado B, la unidad de cuenta utilizada para la determinación de la cuantía de pago de las obligaciones y supuestos previstos por leyes federales que afectan a las entidades y también a la capital, así como en otras disposiciones jurídicas emanadas de las anteriores, será la Unidad de Medida y Actualización (UMA). Dicha reforma señala a la letra:

> El organismo calculará, en los términos que señale la ley, el valor de la Unidad de Medida y Actualización que será utilizada como unidad de cuenta, índice, base, medida o referencia para determinar la cuantía del pago de las obligaciones y supuestos previstos en las leyes federales, de las entidades federativas y del Distrito Federal, así como en las disposiciones jurídicas que emanen de todas las anteriores.
>
> Las obligaciones y supuestos denominados en Unidades de Medida y Actualización se considerarán de monto determinado y se solventarán entregando su equivalente en moneda nacional. Al efecto, deberá multiplicarse el monto de la obligación o supuesto, expresado en las citadas unidades, por el valor de dicha unidad a la fecha correspondiente.

En virtud de lo anterior, el INAI deberá tomar en cuenta la UMA para cuantificar las sanciones y desde luego deberá fundar y motivar sus resoluciones en estricto apego con lo señalado en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, considerando lo siguiente:

1. La naturaleza del dato (cantidad, cualidad, si es sensible o no).
2. La notoria improcedencia de la negativa del responsable, es decir, inexistencia de una causa legítima para declinar una solicitud de derechos ARCO por parte del titular de los datos personales.
3. Carácter intencional de la acción u omisión (elemento volitivo, aunque en ocasiones es difícil de demostrar, probatoriamente hablando).
4. Capacidad económica del responsable, es decir, su aptitud para

[204] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Resoluciones, procedimiento de imposición de sanciones. Expediente: PS.0016/14.

responder frente a las obligaciones nacidas a partir de la verificación de la infracción y la consecuente imposición de la infracción que corresponda por parte del INAI. En este punto se han dado distintas interpretaciones sobre cómo determinar la "capacidad económica del responsable". Hay quienes sostienen que deben tomarse en cuenta los estados financieros del responsable, otros que habría que realizar una auditoría o contar con un dictamen para poder determinarla correctamente.

5. Reincidencia. La repetición sistemática de las conductas consideradas como infracciones sancionables por la Ley y por el propio INAI.

Finalmente, vale la pena señalar que las sanciones se impondrán con absoluta independencia de las responsabilidades civiles o penales a que haya lugar. Separando, de esta forma, las sanciones que son esencialmente de derecho público (en este caso, derecho penal y derecho administrativo) y derecho privado (en este caso, derecho civil). Dejándose a salvo las acciones que el titular de los datos personales violentados pueda ejercer en alguna otra vía ya sea el resarcimiento de los daños y perjuicios o en su caso el daño moral.

Conclusiones

Como hemos podido apreciar a lo largo del presente apartado, son numerosas las faltas que pueden producir sanciones en materia de una indebida protección de datos. La casuística que se presenta sólo es una muestra para evidenciar algunos de los criterios relevantes de la autoridad en la materia y que permiten al lector observar cómo se actualizan en las resoluciones dichas infracciones.

Referencias

García, E. (1998). *Introducción al Estudio del Derecho*. México. Porrúa.

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

INAI. (s.f.). *Resoluciones*. Consultado en: *http://inicio.ifai.org.mx/SitePages/ResolucionesPDP.aspx*

DOF. (2015). *Acuerdo mediante el cual se aprueban los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones*. México.

INAI. (2011). *Guía práctica para la atención de las solicitudes de ejercicios de los derechos ARCO*. México.

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).

CAPÍTULO XI
DE LOS DELITOS EN MATERIA DEL TRATAMIENTO INDEBIDO DE DATOS PERSONALES

CAPÍTULO XI
DE LOS DELITOS EN MATERIA DEL TRATAMIENTO INDEBIDO DE DATOS PERSONALES

Artículo 67. *Se impondrán de tres meses a tres años de prisión al que, estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.*

Artículo 68. *Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.*

Artículo 69. *Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.*

COMENTARIO

Carlos Requena Ochoa

Introducción

Desde el punto de vista del derecho penal es un error común afirmar que los códigos penales y las leyes especiales contienen capítulos en los que se establecen “delitos”. Ese error conceptual tiene su origen en el lenguaje utilizado por el legislador. Así, tenemos que el capítulo XI de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que se comenta, se denomina “De los delitos en materia de tratamiento indebido de datos personales”.

La doctrina especializada coincide en que "delito" es la integración de varios elementos: conducta, tipicidad, antijuridicidad y culpabilidad. Por tanto, las descripciones de conductas que se consideran merecedoras de pena, establecidas en la Ley, no corresponden propiamente a delitos, sino que constituyen, técnicamente, tipos penales.

Incluso, Ernst Beling, quien en 1906 aportó el concepto de "tipicidad" al esquema de la teoría del delito desarrollada por Franz von Liszt, llamó *Tatbestand* a lo que posteriormente se tradujo como "tipo penal", que literalmente significa "supuesto de hecho".[205] Siendo uno de los conceptos más relevantes del derecho penal.

Sin embargo, en este momento no es motivo de reflexión la función que desempeña el tipo penal en la teoría del delito, basta comentar, para efectos del presente análisis, que este concepto corresponde a la descripción que hace el legislador de la conducta, así como de todos los elementos que deben concurrir en su realización, para que aquella resulte penalmente relevante y reprochable. Es decir, coincidimos con quienes afirman que el tipo penal es la descripción que hace el legislador, en la ley, de una determinada conducta antisocial, valorable bajo los principios del derecho penal, con un contenido suficiente y necesario para proteger uno o más bienes jurídicos.

En ese sentido, el ideal de tipo penal que se ha concebido en un Estado de corte democrático es el llamado "tipo cerrado", esto es, el que describe exhaustivamente, con claridad y en todos sus aspectos, el objetivo del deber jurídico penal, traducido en una prohibición o mandato categóricos de orden público. Cuando esto no ocurre, es decir, cuando no está claramente definida la conducta prohibida u ordenada, los tipos penales se conocen como "tipos abiertos".[206]

Un tipo penal con características de "abierto" puede ser cuestionado en su constitucionalidad, en tanto que impide que el ciudadano o destinatario del deber jurídico penal conozca a ciencia cierta cuáles son las conductas prohibidas u ordenadas por la ley. En los tipos penales (materia de la ley federal en comento) consideramos que el legislador no cumple con el principio de legalidad en materia penal,[207] en razón de la forma —no clara— en que los redactó.

[205] Roxin, C. (1997). *Derecho penal, parte general. Fundamentos. La estructura de la teoría del delito.* trad. Diego-Manuel Luzón Peña, Miguel Díaz y García Conlledo y Javier de Vicente Remesal. Madrid. Civitas Ediciones, p. 277.

[206] Ibídem, p. 298.

[207] Véase la jurisprudencia 1a./J. 10/2006. Novena época. Registro 175595, sustentada por la Primera Sala de la Suprema Corte de Justicia de la Nación, visible en el *Semanario Judicial de la Federación* y su gaceta. Tomo XXIII. Marzo de 2006. Materias: Constitucional, Penal, p. 84, de rubro: "Exacta aplicación de la ley penal. La garantía, contenida en el tercer párrafo del artículo 14 de la Constitución Federal, también obliga al legislador".

Genéricamente, se ha identificado que los tipos penales se integran, a su vez, de elementos objetivos, normativos y subjetivos.[208] Los elementos objetivos son aquellos que pueden percibirse a través de los sentidos y tienen cierta materialidad observable. Los normativos corresponden a aquellos vocablos empleados en la descripción del hecho, que deben ser definidos previamente para establecer el contenido y alcances de su significado. Pueden ser de valoración jurídica o cultural.[209] Serán de valoración jurídica cuando el propio orden o sistema normativo proporciona el significado del término y cultural cuando resulta necesario acudir a otra área del conocimiento, distinta del derecho, para delimitarlo.

Los elementos subjetivos hacen referencia a estados psicológicos del sujeto activo en la realización de la conducta delictiva: serán subjetivos genéricos el dolo y la culpa, y subjetivos específicos los distintos del dolo que hacen referencia a ánimos, motivaciones, propósitos o finalidades concretas descritas en el tipo penal. Los elementos subjetivos en su forma genérica, sea dolo y/o culpa, siempre forman parte del tipo penal, pero los elementos subjetivos específicos son "eventuales", pues estos últimos no siempre están necesariamente presentes en las descripciones típicas.

Así, el análisis de un tipo penal puede tomar como punto de partida la identificación de los elementos antes señalados para resolver en cada caso y con la mayor precisión posible, si los hechos acontecidos en la realidad, incluida la conducta probablemente delictiva, colma la posibilidad de ser calificados como delito.

Por la importancia que representa, es necesario hacer referencia a uno de los elementos que resulta común y de mayor relevancia a los tipos penales del capítulo XI de la Ley: el bien jurídico protegido. Este elemento resulta fundamental, pues para que la conducta (acción u omisión) sea considerada delictiva se requiere, necesariamente, que lesione o ponga en riesgo, sin causa justa, al bien jurídico tutelado por el tipo penal.

Análisis de contenido

Bien jurídico protegido

Los tipos penales y el derecho penal en general se justifican en la medida en que tutelan o protegen determinados bienes, intereses o valores que el Estado

[208] Otra forma de clasificación divide a los elementos del tipo penal en: (a) elementos objetivos, que se componen por elementos descriptivos y normativos, respectivamente y (b) elementos subjetivos, que pueden ser genéricos y específicos.

[209] También hay elementos normativos en los tipos penales que hacen más patente la antijuridicidad del comportamiento, por ejemplo: cuando el legislador describe conceptos como: "sin justa causa"; "sin derecho", "indebidamente", entre otros.

considera relevantes para mantener la convivencia ordenada en sociedad, de ahí la necesidad de su tutela penal. El bien jurídico es el elemento rector en la interpretación del tipo penal y es, precisamente, la justificación de la existencia de éste.

Según su relevancia, algunos bienes pueden estar protegidos por otras áreas del orden jurídico, por ejemplo, el derecho administrativo, pues al derecho penal le corresponde —o debería corresponder— sólo a aquellos bienes que sean de tal relevancia que otras áreas del derecho resulten insuficientes o ineficaces para su protección. Al respecto, Reinhart Maurach considera que el derecho penal comparte con las demás ramas del derecho la tarea de protección de la paz jurídica.[210]

Lo anterior cumple —o cumpliría— con principios propios de un Estado democrático (*ultima ratio*, *derecho penal mínimo*, *mínima intervención*), en donde lo que se pretende es limitar, precisamente, el poder punitivo del Estado. Sin embargo, todo dependerá de la política criminal que se asuma como estrategia para combatir el fenómeno delictivo.[211] Es decir, en este caso, para prevenir y erradicar la criminalidad en materia de tratamiento de datos personales.

¿Cómo podemos identificar el bien jurídico protegido por un tipo penal? Los instrumentos del criterio de interpretación sistemático, como son los argumentos: *sedes materiae* y a *rubrica*, respectivamente, resultan de mucha utilidad.[212]

En el caso concreto que nos toca analizar en este apartado, es evidente que los tipos penales se encuentran insertos en una ley especial, cuyo objetivo está precisado en el artículo 1 (argumento *sedes materiae):*

> Artículo 1.- La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la *finalidad* de regular su tratamiento legítimo, controlado e informado, a efecto de *garantizar* la privacidad y el derecho a la autodeterminación informativa de las personas.

Es necesario tener cuidado con el sentido que damos a las palabras utilizadas en la legislación en comento, pues, no obstante que se emplea el vocablo "protección" para referirse a los datos personales en posesión de los particulares, estos últimos no constituyen, en nuestra consideración, el bien jurídico penal tutelado.

[212] Ezquiaga, F. (2006). *La argumentación interpretativa en la justicia electoral mexicana*. México, Tribunal Electoral del Poder Judicial de la Federación, pp. 115 y ss.

Se explica, la ley especial (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) tiene como finalidad regular el tratamiento legítimo, controlado e informado de los datos personales en posesión de los particulares a partir de su protección. Sin embargo, esa regulación tiene un objetivo mayor que se hace explícito en el propio artículo: garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Si atendemos a la denominación del capítulo XI de la ley, que trata sobre los delitos en materia de tratamiento indebido de datos personales, podemos advertir que las conductas que se consideran delictivas se vinculan, precisamente, con el tratamiento indebido (argumento "a rubrica").

En este sentido, es el tratamiento indebido el que vulnera los bienes jurídicos protegidos en los tipos penales, específicamente: la privacidad y la autodeterminación informativa de las personas. No consideramos que sean los datos personales, en sí mismos, los que se vulneran por el delito, pues no representan *per se* algún valor susceptible de tutela por parte del derecho penal. Los datos personales o las bases de datos, en realidad, constituyen únicamente el objeto material sobre el que recae la conducta típica penal.

En efecto, la doctrina penal coincide en que el objeto material, como elemento del tipo penal, es el ente corpóreo (persona o cosa) sobre el cual recae o se realiza la conducta del sujeto activo que, al verse concretado, genera la lesión o puesta en peligro al bien jurídico protegido.

Es importante mencionar que la protección de los datos personales (entendida como esa función de regular su tratamiento legítimo, controlado e informado) se realiza por otra área del derecho: el administrativo, y sólo cuando se lleva a cabo algún tratamiento indebido de esos datos, es que se justifica la intervención del derecho penal, al lesionarse o ponerse en peligro la privacidad y/o la autodeterminación informativa de las personas.

De ahí que los bienes jurídicos tutelados por los tipos penales son mencionados por la ley (la privacidad y/o la autodeterminación informativa de las personas), pero no los datos personales, que constituyen, únicamente, el objeto material sobre el que recae la conducta típica. Ciertamente, la protección de los datos personales, en sí misma, es propia del derecho administrativo.

Sin embargo, hay quienes pudieran considerar la necesidad de hacer más extensiva la interpretación de la política criminal que subyace en la creación de los tipos penales establecidos en la Ley para también considerar, penalmente,

como bien jurídico protegido, la debida protección de los datos personales en posesión de los particulares, pero esto es materia de controversia.

En realidad, la discusión sobre qué bienes jurídicos son protegidos por los tipos penales en comento, desde el punto de vista penal, invita a analizar si estamos en presencia de un expansionismo del derecho penal, el cual pretende absorber materias y capítulos enteros del derecho administrativo sancionador, así como del derecho privado.

Tipos penales

Los tipos penales se encuentran previstos en el citado capítulo XI de la ley especial en comento, específicamente en los artículos 67 y 68, pues como se verá más adelante, el artículo 69 se refiere sólo a una circunstancia agravante de la pena (agravante de la punibilidad) prevista en los tipos penales básicos (artículos 67 y 68).

El análisis hace necesaria su transcripción literal:

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

Análisis del tipo penal previsto en el artículo 67

Identificación de la conducta típica

En derecho penal, una conducta puede ser entendida como acción u omisión. La primera se concibe, en el sistema clásico de la teoría del delito, como un movimiento corporal voluntario (actividad o inactividad) que produce un cambio en el mundo de la realidad. Un nexo de causalidad une el movimiento con el resultado. Esta última es la razón por la que al sistema clásico —de manera poco afortunada— también se le conoce como sistema causalista.[213]

Por su parte, con la teoría de la acción finalista del derecho penal, que en la actualidad es la de mayor influencia en la legislación penal mexicana, la acción

[213] Díaz, E. (2006). *Teoría del delito (doctrina, jurisprudencia y casos prácticos)*. México. Straf, p. 21.

humana se concibe como un ejercicio de actividad final. Es decir, un obrar orientado conscientemente desde un fin.[214] Recordemos que nuestro Código Penal Federal, en su artículo 8 dispone que las acciones u omisiones delictivas unicamente pueden realizarse dolosa o culposamente. La exposición anterior es solo un panorama genérico, que no exhaustivo, acerca de la conducta como un elemento del delito.

En el caso concreto, la conducta que prevé el tipo penal del artículo 67 se puede identificar conl verbo rector "provocar". El diccionario de la RAE define dicha palabra en la primera de sus acepciones como producir o causar algo. Ese algo que se causa o produce debe ser una vulneración de seguridad, según describe el tipo penal.

Antes de continuar advertimos un problema: ¿cómo se puede producir o causar algo? Sin duda, mediante una acción o una omisión humana. Entonces, tal parece que el tipo penal no define con claridad cuál es la conducta prohibida, ya que alguien puede provocar el resultado exigido por el tipo penal si realiza determinada actividad o si deja de realizarla.

No es posible determinar, en tal sentido, cuál es la verdadera conducta merecedora de pena, lo que —aparentemente— resulta contrario al principio de "exacta aplicación" de la ley que también obliga al legislador, ya que se puede llegar a afirmar la realización de la conducta por el sólo hecho de haber contribuido con alguna condición —por mínima que sea— para generar la vulneración de seguridad exigida por el tipo penal descrito en el artículo 67.

Por tal motivo, es cuestionable —con base en el principio de legalidad— que la conducta sea identificada genéricamente como "provocar", pues resultaría tan amplia que cualquier acción u omisión podría estimarse como causante del resultado, sin estar específica o claramente descrita por el tipo penal.

No obstante, en la práctica, el tipo penal se resuelve satisfactoriamente si interpretamos que contiene un deber jurídico penal, consistente en la prohibición de provocar "con ánimo de lucro, una vulneración de seguridad a las bases de datos, bajo su custodia, estando autorizado para tratar datos personales".[215] Es decir, bastaría cualquier comportamiento que, a fin de cuentas, resultara idóneo para concretar los elementos objetivos del tipo penal. Por ejemplo, en el caso del tipo penal de homicidio (artículo 302 del Código Penal Federal, CPF), el legislador no describe todas las formas o comportamientos para privar de la vida a otra persona. Asimismo, en el tipo de daño en propiedad ajena (artículo 397 del CPF) tampoco se describe todas las formas de causar daños.

[214] Welzel, H. (1997). *Derecho penal alemán.* Trad. Juan Bustos Ramírez y Sergio Yañez Pérez. Santiago de Chile. Editorial Jurídica de Chile, pp. 39 y ss.
[215] Artículo 67 de la Ley Federal de Protección de Datos en Posesión de los Particulares.

Regresando al análisis del tipo penal del artículo 67 de la Ley, si provocar significa producir o causar algo, ese algo, conforme a la redacción del tipo penal, debe ser una vulneración de seguridad a las bases de datos bajo su custodia.

En este sentido, vulneración de seguridad constituye un elemento normativo de valoración jurídica, pero adviértase que los alcances de su significado los proporciona el reglamento de la Ley. Es decir, a nivel de una norma de menor jerarquía, como la reglamentaria, se delimitan expresa y normativamente los supuestos que constituyen una vulneración de seguridad, para los efectos del tipo penal del artículo 67.

El artículo 63 del citado reglamento dispone:

> Artículo 63. Las *vulneraciones de seguridad* de datos personales ocurridas en cualquier fase del tratamiento son:
> I. La pérdida o destrucción no autorizada.
> II. El robo, extravío o copia no autorizada.
> III. El uso, acceso o tratamiento no autorizado.
> IV. El daño, la alteración o modificación no autorizada. (Énfasis añadido).

Este tipo penal nos plantea un problema de constitucionalidad de las denominadas leyes penales en blanco. Al respecto, es necesario mencionar que este problema no se plantea cuando la norma penal remite a otra de naturaleza extrapenal en sentido formal y material (para quedar plenamente integrada), sino únicamente cuando se reenvía a otra norma que no tiene el carácter de ley en sentido formal, dando así entrada en la descripción típica a regulaciones de procedencia reglamentaria o hasta meramente administrativa y, en consecuencia, a una participación del Poder Ejecutivo en la configuración de los tipos penales.[216]

Adicionalmente, la Primera Sala de la Suprema Corte de Justicia de la Nación ha definido los tipos penales en blanco como los hipotéticos supuestos en los que la conducta delictiva se precisa en términos abstractos y requiere de un complemento para integrarse plenamente, los cuales son inconstitucionales si su integración debe realizarse mediante la remisión a normas reglamentarias, pues ello equivale a delegar a un poder distinto al legislativo —en este caso al Poder Ejecutivo Federal— la potestad de intervenir decisivamente en la determinación del ámbito penal, cuando es facultad

[216] Leyes penales en blanco. Problemática de constitucionalidad de aquéllas. Tesis: Décima Época, Registro: 2011281. Instancia: Primera Sala. Tipo de Tesis: Aislada. Fuente: *Gaceta del Semanario Judicial de la Federación*. Libro 28, marzo de 2016. Tomo I. Materia(s): Constitucional. Tesis: 1a. LXXII/2016 (10a.), p. 987.

exclusiva e indelegable del Congreso de la Unión legislar en materia de delitos y faltas federales.[217]

Este cuestionamiento resulta trascendente para efectos penales, también frente a un importante criterio jurisprudencial de la Segunda Sala al señalar que, según ha sostenido este alto tribunal en numerosos precedentes, el artículo 89, fracción I, constitucional, faculta al presidente de la República para expedir normas reglamentarias de las leyes emanadas del Congreso de la Unión y, aunque desde el punto de vista material ambas normas son similares, aquéllas se distinguen de éstas, básicamente, en que provienen de un órgano que al emitirlas no expresa la voluntad general, sino que está instituido para acatarla en cuanto dimana del Legislativo, de donde, por definición, son normas subordinadas, de lo cual se sigue que la facultad reglamentaria se encuentre regida por dos principios: el de reserva de ley y el de subordinación jerárquica a la misma. El principio de reserva de ley, que desde su aparición como reacción al poder ilimitado del monarca hasta su formulación en las constituciones mo-dernas, ha encontrado su justificación en la necesidad de preservar los bienes jurídicos de mayor valía de los gobernados (tradicionalmente libertad personal y propiedad), prohíbe al reglamento abordar materias reservadas en exclusiva a las leyes del Congreso, como son las relativas a la definición de los tipos penales, las causas de expropiación y la determinación de los elementos de los tributos, mientras que el principio de subordinación jerárquica, exige que el reglamento esté precedido por una ley cuyas disposiciones desarrolle, complemente o pormenorice y en las que encuentre su justificación y medida.[218]

A diferencia del concepto anterior (vulneraciones de seguridad), la referencia textual al concepto: bases de datos, que también constituye un elemento normativo de valoración jurídica en el tipo penal del artículo 67, sí encuentra su definición en el artículo 3, fracción II de la Ley:

> Artículo 3.- Para los efectos de esta Ley, se entenderá por:[…] II. *Bases de datos:* El conjunto ordenado de datos personales referentes a una persona identificada o identificable. (Énfasis añandido).

En atención a las definiciones proporcionadas por la legislación aplicable, es posible afirmar —haciéndose explícitos los significados— que la conducta prevista en el tipo penal del artículo 67 consiste en:

---

[217] Tipos administrativos en blanco. Son constitucionales si se justifican en el modelo de Estado regulador. Tesis: Décima Época. Registro: 2007412. Instancia: Primera Sala. Tipo de Tesis: Aislada. Fuente: *Gaceta del Semanario Judicial de la Federación*. Libro 10, septiembre de 2014. Tomo I. Materia(s): Constitucional. Tesis: 1a. CCCXIX/2014 (10a.), p. 592.

[218] Facultad reglamentaria del presidente de la República. Principios que la rigen. Época: Novena Época. Registro: 194159. Instancia: Segunda Sala. Tipo de Tesis: Jurisprudencia. Fuente: *Semanario Judicial de la Federación* y su Gaceta. Tomo IX. Abril de 1999. Materia(s): Constitucional. Administrativa. Tesis: 2a./J. 29/99, p. 70.

> Al que (estando autorizado para tratar datos personales, con ánimo de lucro), produzca o cause (provoque) la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada (una vulneración de seguridad) al conjunto ordenado de datos personales referentes a una persona identificada o identificable (a las bases de datos), bajo su custodia.

La anterior conclusión nos lleva a afirmar que este tipo penal exige, en la mayoría de los supuestos, la producción de un resultado material. Hablamos, en tal sentido, de un delito de daño y no sólo de puesta en peligro o riesgo del bien jurídico tutelado. El derecho penal considera que el resultado material es el efecto o consecuencia natural de la conducta que realiza el sujeto activo.

Para el ingeniero Ubaldo Martínez Eslava, perito en informática, provocar una vulneración de seguridad significa encauzar el aprovechamiento de debilidades de diseño o error de implementación de las bases de datos para generar un evento inesperado donde se comprometa la seguridad física o lógica. Destaca —como un tema de gran importancia— que este tipo penal del artículo 67 únicamente contempla la seguridad de las bases de datos. Sin embargo, pudiera haber circunstancias donde no se comprometa la seguridad de las bases de datos, pero sí la seguridad de la información, que tiene como componentes la disponibilidad, confidencialidad e integridad.[219]

Citemos el ejemplo de cómo una persona, ajena al tratamiento de datos, que conoce por algún medio o circunstancia las credenciales de acceso a las bases donde se resguarda información personal, en cualquier momento puede hacer uso de ellas e ingresar a la base de datos comprometiendo la disponibilidad, confidencialidad e integridad de la información personal. En este caso, dicho acceso no puede ser considerado una vulneración de seguridad de las bases de datos, puesto que la persona que ingresa a dicha base no aprovechó una debilidad de diseño o implementación, tampoco evadió o violentó las medidas físicas o lógicas que protegen la seguridad y sin embargo, sí comprometió la disponibilidad, confidencialidad e integridad de la información contenida. Es decir, el legislador no consideró a aquella persona que no se encuentra autorizada para tratar datos personales, pero que sí puede comprometer la seguridad de las bases de datos o la de la información. Este es un aspecto que no consideró el legislador.

[219] Disponibilidad: refiere al hecho de que la información se encuentre lista para su consulta en todo momento. Confidencialidad: refiere a la secrecía de la información contenida en la base de datos. Integridad: refiere a la veracidad de la información, o que la información sea fiable y se mantenga sin alterar.

Calidad específica del sujeto activo

La conducta descrita en el artículo 67 no puede ser ejecutada por cualquier persona física. Nótese que el tipo penal exige que la lleve a cabo quien está autorizado para tratar datos personales y tiene bajo su custodia las bases de datos de que se trata.

Al respecto, la Ley, en su artículo 3, da cuenta del significado de los siguientes términos:

> Artículo 3.- Para los efectos de esta Ley, se entenderá por:
> […] V. Datos personales: Cualquier información concerniente a una persona física identificada o identificable.
> […] IX. Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.
> […] XIV. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.
> […] XVI. Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.
> XVII. Titular: La persona física a quien corresponden los datos personales.
> XVIII. Tratamiento: 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.
> XIX. Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.
> Como se puede observar, los conceptos empleados en el tipo penal, y que constituyen elementos normativos, son definidos por el legislador en la propia Ley. Son pues, elementos normativos de valoración jurídica descritos en el tipo penal.

Recordemos que calidad específica del sujeto activo del delito es[220] el conjunto de características exigidas en el tipo penal y que delimitan a los sujetos a quienes va dirigido el deber jurídico penal. En ese sentido, la calidad específica que se exige del sujeto activo, como la persona autorizada para tratar datos personales, se puede identificar tanto en el responsable como en el encargado, incluso, en algunos supuestos, en el tercero.

Esto último se afirma porque los artículos 21 y 36 de la Ley prevén supuestos en los cuales los terceros pueden intervenir en el tratamiento de datos personales:

[220] En términos de la doctora Olga Islas.

> Artículo 21. El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.
> Artículo 36.- Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.
> El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

Por otra parte, con relación al elemento normativo consistente en "bajo su custodia", el artículo 47 del reglamento de la Ley hace una referencia a dicho vocablo cuando define el principio de responsabilidad en materia de protección de datos:

> Principio de responsabilidad.
>
> Artículo 47. En términos de los artículos 6 y 14 de la Ley, el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano.
> Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.

Al respecto, podría concluirse que los datos personales están bajo custodia de una persona cuando los ha obtenido legalmente para su tratamiento o le han sido transferidos bajo un título legítimo.

Una crítica importante radica en que el tipo penal analizado del artículo 67 no considera los casos en los que personas no autorizadas para tratar datos personales pueden comprometer la seguridad de las bases de datos. Estos casos, técnicamente, serían calificados como conductas atípicas que excluyen el delito, atendiendo al texto del artículo 67, lo que sin duda también merece una urgente atención legislativa.

Pero si con base en los hechos de esos posibles casos no es posible encuadrar la conducta probablemente constitutiva de delito por demostrarse

la inexistencia de alguno de los elementos que integran la descripción típica del delito de que se trate, habrá de realizar un diverso ejercicio de tipicidad con base en otros tipos penales, específicamente los contenidos en el CPF, capítulo II, título noveno, relativos al acceso ilícito a sistemas y equipos de informática, con el objetivo de analizar los elementos, por ejemplo, del artículo 211 bis 1.[221]

Elemento subjetivo específico

La conducta que se analiza, descrita en el artículo 67, debe realizarse con ánimo de lucro. Este elemento subjetivo específico —distinto del dolo de la conducta como elemento subjetivo genérico— implica que el sujeto activo tiene la intención o propósito específico de obtener una ganancia o provecho con motivo de la conducta realizada. La descripción del tipo penal implica que no se requiere la necesaria o efectiva obtención de la ganancia, pues la tipicidad se colma y actualiza con el sólo ánimo, propósito o intención de obtenerla.

Esto nos lleva a determinar que la conducta analizada en el tipo penal del artículo 67 es eminentemente dolosa, pues no prevé la realización por culpa. Por tanto, si alguien por imprudencia, negligencia o falta de cuidado provoca una vulneración de seguridad a las bases de datos, no actualizaría la conducta típica descrita en el tipo penal.

Recordemos que el delito se excluye, entre otras cuestiones, cuando se demuestra la inexistencia de alguno de los elementos que integran la descripción típica del delito de que se trate, como por ejemplo: el elemento subjetivo genérico dolo (artículo 15, fracción III del Código Penal Federal).

Pero, ¿qué sucede en los casos en que, sin ánimo de lucro, se compromete la seguridad a las bases de datos? Un supuesto no regulado ni previsto por el legislador que, sin duda, resulta relevante, ya que sin ese ánimo de lucro la conducta no podría ser calificada como típica ni delictiva, pese a la producción del resultado, precisamente ante la falta del elemento subjetivo específico apuntado (sin ánimo de lucro).

Indudablemente, una conducta, aún sin ánimo de lucro, también puede provocar un daño e, inclusive, un riesgo para el titular de los datos. Un ejemplo de lo anterior es la vulneración de información relativa a la creencia, inclinación o preferencia sexual o situación médica, con el simple hecho de publicarla sin ánimo de lucro, violentaría datos sensibles del titular por parte del sujeto obligado o autorizado para tratar dichos datos personales.

[221] Artículo 211 bis del CPF: “Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa”.

En nuestra consideración, el legislador describe en el tipo penal del artículo 67 una calidad de garante en el sujeto activo cuando exige que quien provoque una vulneración de seguridad a las bases de datos, las tenga bajo su custodia.

De acuerdo con la Dra. Olga Islas definimos la calidad de garante como un elemento del sujeto activo en el tipo penal, como: "La relación especial, estrecha y directa en que se encuentra un sujeto activo y un bien jurídico singularmente determinado, para la salvaguarda, custodia o protección efectiva de dicho bien jurídico protegido". Nótese que la Ley hace énfasis respecto del responsable, quien tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión. Esto significa que surge esa relación entre la persona autorizada para tratar datos personales y la privacidad y/o la autodeterminación informativa de las personas.

Adicionalmente, el tipo penal que se analiza describe una referencia de ocasión, es decir, una situación especial generadora del riesgo para el bien jurídico protegido, la cual es aprovechada (dolosamente) por el sujeto activo para realizar la conducta o producir el resultado. En este caso, el sujeto autorizado para tratar datos personales se encuentra en custodia de los datos personales y, a sabiendas de su posición de salvaguarda, la aprovecha provocando una vulneración de seguridad a las bases de datos que están bajo su custodia.

El tipo penal del artículo 67 no exige para su comisión o actualización (para la realización de la conducta) algún medio comisivo específico, ni que se lleve a cabo en determinadas circunstancias exigibles de tiempo o lugar.

Podemos concluir que la descripción del tipo penal del artículo 67 prevé la imposición de pena de prisión al responsable, encargado o tercero (autorizado) que, con la intención específica de obtener una ganancia o provecho (ánimo de lucro) produzca, cause o provoque —dolosamente— la destrucción, pérdida, robo, extravío, copia, uso, acceso, tratamiento, daño, alteración o modificación no autorizadas (vulneración de seguridad) al conjunto ordenado de datos personales referentes a una persona identificada o identificable (a las bases de datos), que legalmente ha obtenido o le ha sido transferida para su tratamiento (bajo su custodia).

Para invitar al debate y deliberación, desde el punto de vista de la seguridad de la información, sugerimos una enmienda a la redacción del tipo penal, a fin de considerar una futura reforma legislativa al artículo 67:

Texto actual del artículo 67	Texto que se sugiere
Con ánimo de lucro.	Con o sin ánimo de lucro.
Provoque una vulneración de seguridad a las bases de datos bajo su custodia.	Provoque una vulneración de seguridad de la información de las bases de datos bajo su custodia.

Esta propuesta también puede aplicarse en el artículo 63 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, al referirse a las vulneraciones de seguridad de datos personales.

Es necesario que el legislador, al momento de redactar los tipos penales, considere el entendimiento y armonización normativa con el lenguaje propio de las TIC que involucra también a la informática forense, la seguridad y gobierno de la información.

Los siguientes conceptos son un ejemplo:

Vulneración: aprovechamiento de una debilidad de diseño o implementación de un sistema o base de datos para generar un evento inesperado que comprometa la seguridad del sistema.

Seguridad de las bases de datos: relativa a las medidas o mecanismo de seguridad físicos o lógicos que protejan la información de las bases de datos (biométricos, de sistemas de autentificación de contraseñas, antivirus, de sistemas de detección de intrusos (IDS), *firewall*, etc.

Seguridad de la Información: relativa a mantener íntegros los componentes de disponibilidad, confidencialidad e integridad.

Análisis del tipo penal previsto en el artículo 68

Identificación de la conducta típica

En el caso concreto, la conducta que prevé el tipo penal del artículo 68 está identificada en el verbo rector “tratar”. Este vocablo, así como “datos personales”, es definido por la Ley:

> Artículo 3.- Para los efectos de esta Ley, se entenderá por:
> […] V. Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

> […] XVIII. Tratamiento: 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.

A partir de las definiciones legales citadas (elementos normativos de valoración jurídica) se puede determinar que la conducta prevista por este tipo penal se actualiza cuando una persona física obtenga, acceda, maneje, aproveche, transfiera, disponga, divulgue, almacene o trate, por cualquier medio, información concerniente a una persona física identificada o identificable (datos personales).

Tal y como en el caso del tipo penal analizado previamente del artículo 67, podemos afirmar que también se exige la producción de un resultado material, ya que se trata también de un delito de daño y no sólo de puesta en peligro o riesgo del bien jurídico tutelado.

Calidad específica del sujeto pasivo

A diferencia del tipo penal anterior (artículo 67), en este caso (artículo 68) no se exige una calidad específica en el sujeto activo, es decir, no se prevé que deba estar autorizado para tratar datos personales, por ende, puede ser cometido por cualquier persona física imputable. Recordemos que la imputabilidad, en el derecho penal, es la capacidad del sujeto activo para comprender la ilicitud de su conducta.

No obstante, el tratamiento de datos personales en el tipo penal del artículo 68 que se analiza, como se verá, exige su realización mediante "el engaño, aprovechándose del error en que se encuentra el titular o la persona autorizada para transmitirlos".[222] En consecuencia, exige un medio de comisión expresamente descrito, pues si se lleva a cabo en ese contexto, es evidente que quien desarrolla la conducta no está autorizado, legalmente, para tratar datos personales.

Entendemos que esta es la razón del legislador para que, conforme a la política criminal que consideró más conveniente, elevara la pena tratándose del tipo penal del artículo 68 (de seis meses a cinco años de prisión) con relación al artículo 67 que establece una sanción menor (de tres meses a tres años de prisión).

Siguiendo con el análisis y con relación al sujeto pasivo, el tipo penal exige que sea el titular o la persona autorizada para transmitir los datos personales. Al respecto, la ley federal en comento prevé:

[222] Artículo 68 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

> Artículo 3.- Para los efectos de esta Ley, se entenderá por:
> XVII. Titular: La persona física a quien corresponden los datos personales.

En consecuencia, será sujeto pasivo del delito sólo la persona a quien corresponden los datos personales o quien está autorizada para transmitirlos.

En el derecho penal, la doctrina dominante afirma que será sujeto pasivo el titular del bien jurídico protegido en el tipo penal. En este caso es el titular de la privacidad y/o la debida protección de los datos personales. Será sujeto pasivo quien concrete la ofensa o agravio reprochable por el derecho penal.

Elemento subjetivo específico

En el caso del tipo penal del artículo 68, la conducta debe realizarse con el fin de alcanzar un lucro indebido. Este elemento subjetivo específico —distinto del dolo— también implica que el sujeto activo tenga la intención o propósito específico de alcanzar una ganancia o provecho indebido con motivo de la conducta realizada. Ese fin ilícito complementa la conducta del sujeto activo, la cual debe realizarla en forma dolosa ya que, conociendo los elementos del tipo penal o previendo, como posible el resultado típico, quiere o acepta la realización del hecho descrito por la ley con el fin indebido. Por tanto, para la actualización o concreción del delito, siempre debe realizar su conducta en forma dolosa.

Es importante aclarar que, cuando en el tipo penal (artículo 68) se describe que el lucro debe ser indebido, no supone que en el diverso tipo penal (del artículo 67) no lo sea, a pesar de que en éste se exige que la conducta se realice solo “con ánimo de lucro”. En efecto, pues lo indebido, ilegal o contrario a derecho es una característica de la conducta que, aunque no se describe expresamente en el texto del tipo penal (artículo 67), sí debe analizarse —tal conducta— también a nivel de la antijuridicidad.

La naturaleza de la conducta, descrita en el tipo penal del artículo 68, no prevé la forma de realización por culpa, lo que significa que no se puede engañar mediante imprudencia, negligencia o falta de cuidado. Además, este tipo penal no permite la comisión culposa por no estar previsto en las reglas del catálogo del artículo 60 del CPF, ni estar, expresamente, permitido por la propia Ley.

Medios comisivos específicos

Este tipo penal, a diferencia del artículo 67, exige para su actualización que la conducta se realice a través de un medio comisivo específico: el engaño.

Al respecto, el propio reglamento de la Ley se encarga de definir qué se entiende por actuación engañosa:

> Artículo 44. El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, en los términos establecidos en el artículo 7 de la Ley.
> No se podrán utilizar medios engañosos o fraudulentos para recabar y tratar datos personales. Existe una *actuación fraudulenta o engañosa* cuando:
> 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 a la que refiere el artículo 7 de la Ley, o
> III. Las finalidades no son las informadas en el aviso de privacidad.

Conforme a una interpretación estricta del tipo penal del artículo 68, el tratamiento de los datos personales debe, necesariamente, darse en alguno de los supuestos señalados para afirmar que se realizó mediante engaño del sujeto activo.

Sin embargo, la única precisión, desde el punto de vista penal, es la relativa a que debe excluirse el supuesto o caso de negligencia como medio comisivo del delito, toda vez que el tipo penal, como ya se señaló, exige una actuación necesariamente dolosa, acorde con las reglas y principios interpretativos del derecho penal, así como con la naturaleza de la conducta delictiva propia del tipo penal del artículo 68.

El ingeniero Ubaldo Martínez Eslava destaca que en el campo de la informática forense la palabra “engaño” se relaciona con la utilización de las técnicas conocidas como *phishing* e ingeniería social. La primera (*phishing*) se refiere a la técnica que aprovecha la confusión del custodio o titular para obtener información de datos personales, financieros o credenciales de acceso a sistemas o bases de datos utilizando información apócrifa o falsa como son páginas *web*, correos electrónicos, mensajes SMS/MMS, llamadas telefónicas, infección de *malware*, etc. La segunda (ingeniería social) se refiere al arte de convencer a las personas para que revelen información utilizando como factor el hecho de que la gente desconoce la importancia de la información o es descuidada en su protección.

Al respecto, es de destacarse que la legislación federal en comento no hace referencia a este tipo de técnicas, lo que puede considerarse falta de actualización en el lenguaje utilizado por el legislador para describir el tipo penal en esta ley especial. Sin una armonización del campo de seguridad de

la información con los tipos penales, se dificultará la comunicación entre las áreas legales y técnicas al momento de aplicar la ley a casos reales.

No se soslaya que el tipo penal prevé el aprovechamiento del error en que se encuentra el titular o la persona autorizada para trasmitir los datos personales. La expresión "…mediante el engaño, aprovechándose del error en que se encuentre el titular…" es una oración yuxtapuesta formada por dos partes "engaño" y "aprovechándose del error". Ambas proposiciones cuentan consentido completo, es decir, podrían entenderse aun cuando aparezcan aisladas. Sin embargo, la "coma" en el tipo penal (artículo 68) permite realizar la yuxtaposición y dar forma a la oración reunida.

Parecería que, por virtud de la interpretación estricta que rige en el derecho penal, no se permite aplicar o entender las dos frases "engaño" y "aprovechándose del error" como independientes, sino al ser marcadas por el nexo gráfico (la coma) conforma una oración compuesta y no dos oraciones separadas. Esta redacción parece responder a una deficiente técnica legislativa, más que a cuestiones de estilo o semánticas.

Luego entonces, los dos supuestos descritos en el tipo penal del artículo 68 son:

a) El engaño, como medio comisivo del sujeto activo, que debe ser exteriorizado para provocar la falsa apreciación de la realidad en el sujeto pasivo.
b) La preexistencia del error en que se encuentra el titular o la persona autorizada para transmitir datos personales, situación que es aprovechada por el sujeto activo. En este supuesto, la falsa apreciación de la realidad en el sujeto pasivo acontece en sí misma y previamente, sin que el sujeto activo lleve a cabo algún ardid, maquinación o artificio para provocar ese estado de error. No obstante, este estado del sujeto pasivo es advertido por el sujeto activo y, por ende, dolosamente aprovechado.

La redacción del tipo penal (artículo 68) no es clara.

Parece que no existe duda en la actualización de la conducta en la primera hipótesis (a), cuando el sujeto activo, mediante el engaño, provoca el error y se aprovecha de él.

La duda se presenta en el segundo supuesto (b), en casos donde el sujeto activo solo se aprovecha del error en que se encuentra el titular, pero sin ejecutar algún ardid, maquinación o artificio para provocar dicho estado de error. En estos casos podría alegarse excluyente de delito por atipicidad

en la conducta, pues el tipo penal exige también, tal y como está redactado, un medio comisivo específico consistente en el engaño, precisamente para el acto de aprovecharse del error en que se encuentra el titular o la persona autorizada para transmitir los datos personales.

Pero mantener separados los dos supuestos no resulta posible según la descripción textual del tipo penal (yuxtaposición). A pesar de ello, no descartamos hechos de la realidad donde puedan actualizarse los dos supuestos típicos, por ejemplo, cuando el titular o la persona autorizada para transmitir datos personales cae en el estado de error (previamente y por causas ajenas al sujeto activo), pero éste, al percatarse de dicho estado de error del titular decide tratar datos personales, llevando a cabo o exteriorizando dolosamente un engaño, ardid, maquinación o artificio, con el fin de alcanzar un lucro indebido.

El legislador debió prever supuestos redactados con mayor claridad, tendientes a proteger, en forma más efectiva, los bienes jurídicos resguardados por el tipo penal: la privacidad y la autodeterminación informativa de las personas, respectivamente.

Este tipo penal del artículo 68 no exige, para su actualización, que la conducta del sujeto activo se realice en determinadas circunstancias de lugar, tiempo, modo u ocasión.

El tipo penal del artículo 68 prevé la imposición de una pena a quien, con la intención o propósito específico de alcanzar una ganancia o provecho indebido, obtenga, acceda, maneje, aproveche, transfiera, disponga, divulgue o almacene, por cualquier medio, información concerniente a una persona física identificada o identificable, mediante una actuación engañosa (de las previstas en el artículo 44 del reglamento), aprovechándose del error (la falsa apreciación de la realidad) en que se encuentra la persona física a quien corresponden los datos personales o la autorizada para transmitirlos.

Para invitar al debate y deliberación, desde el punto de vista de la seguridad de la información, pudiéramos sugerir una enmienda a la redacción del tipo penal, a fin de considerar una futura reforma legislativa al artículo 68:

Texto actual del artículo 68	Texto que se sugiere
Mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.	Mediante el engaño, o aprovechándose del error o descuido en que se encuentre el titular o la persona autorizada para transmitirlos.

Análisis de la circunstancia agravante prevista en el artículo 69

El artículo 69 no prevé un tipo penal, sino que contempla, únicamente, una circunstancia agravante para los tipos penales básicos descritos en los artículos 67 y 68. Señala que, si las conductas previstas en esos artículos se realizan respecto de datos personales sensibles, las penas se duplicarán.

La Ley define "datos personales sensibles" de la siguiente forma:

> Artículo 3.- Para los efectos de esta Ley, se entenderá por:
> […] VI. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Nótese que, si el tipo penal del artículo 67 contempla un rango o intervalo de punibilidad de tres meses a tres años de prisión y el tipo penal del artículo 68, de seis meses a cinco años de prisión, es evidente que, de actualizarse la circunstancia agravante exigida por el artículo 69, la pena privativa de libertad quedaría conformada con nuevos rangos de punibilidad, duplicados: de seis meses a seis años para el primero (artículo 67) y de uno a diez años para el segundo (artículo 68).

En toda circunstancia agravante es necesario que el legislador justifique la punibilidad prevista en la norma, con base en una política criminal coherente y consistente o, en su caso, con una exposición de motivos clara. Lo anterior, para no dejar, como parecería en el caso del artículo 69, ambigüedades de criterio por falta de objetividad para determinar el merecimiento de pena de prisión duplicada por lesionarse determinados bienes jurídicos protegidos de mayor jerarquía o valor.

Si, como se ha expuesto en estos comentarios, entendemos que los bienes jurídicos protegidos por los tipos penales del capítulo XI (De los Delitos en Materia del Tratamiento Indebido de Datos Personales) de la Ley, consisten en la privacidad y la autodeterminación informativa respectivamente, será cuando el objeto material recaiga en datos personales sensibles, que se actualiza la circunstancia agravante. Es decir, tratándose de datos personales sensibles, los bienes jurídicos protegidos adquieren más relevancia, lo que parece justificar que estamos ante bienes jurídicos de mayor jerarquía o valor, específicamente: la privacidad íntima y la autodeterminación informativa íntima de las personas. Es decir, la intimidad.

La relevancia del reproche y castigo penal de un comportamiento humano, descrito en un tipo penal, depende de la falta de valor de la conducta realizada, dejándose a las consideraciones de la política criminal legislativa laconveniencia de castigarla con mayor severidad. Incluso, el artículo 22 de la Constitución establece que: "Toda pena deberá ser proporcional al delito que sancione y al bien jurídico afectado".

En consecuencia, la esfera íntima del titular de los datos personales sensibles los convierte en datos personalísimos y relevantes para el derecho penal, los cuales, ante su tratamiento o uso indebido, según el enfoque basado en riesgo que previene el legislador en la Ley (concretamente, poder dar origen a discriminación o conllevar un riesgo grave para el titular) justifican también el agravante, duplicando el rango o intervalo de punibilidad de la pena de prisión.

Conclusiones

Advertimos la importancia del principio de responsabilidad establecido en el artículo 47 de la ley en comento y su relación con el *compliance* o cumplimiento regulatorio. El legislador, en esta ley especial, otorga la posibilidad normativa para que el responsable de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, pueda valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines. Es decir, valerse del *soft law* o de cualquier legítima regulación suave.

Esta importante "posibilidad normativa" abre la puerta para analizar, en un futuro muy cercano, si con base en una política criminal relacionada con los "delitos en materia del tratamiento indebido de datos personales" cometidos en el seno de las personas jurídicas, se justifica que los tipos penales de los artículos 67 y 68 de la ley se añadieran o integraran al catálogo del artículo 11 bis del Código Penal Federal (CPF) para posibilitar la responsabilidad penal a dichas personas jurídicas.

El artículo 11 bis del CPF señala:

> Para los efectos de lo previsto en el Título X, Capítulo II, del Código Nacional de Procedimientos Penales, a las personas jurídicas podrán imponérseles algunas o varias de las consecuencias jurídicas cuando hayan intervenido en la comisión de los siguientes delitos [...] En todos los supuestos previstos en el artículo 422 del Código Nacional de Procedimientos Penales, las sanciones podrán atenuarse hasta en una cuarta parte, si con anterioridad al hecho que se les imputa, las personas jurídicas contaban con un órgano de control permanente, encargado de verificar el cumplimiento de las disposiciones legales aplicables

> para darle seguimiento a *las políticas internas de prevención delictiva* y que hayan realizado antes o después del hecho que se les imputa, la disminución del daño provocado por el hecho típico. (Énfasis añadido).

Este debate o análisis —eventualmente justificativo— resulta necesario ante la tendencia regulatoria mundial del *compliance* y la responsabilidad legal de las personas jurídicas en México, máxime si tomamos en cuenta que, generalmente, las personas que más acopian información, requieren mayor seguridad para custodiar sus bases de datos y la información que resguardan. Además, las personas jurídicas, específicamente las empresas, son las que reúnen más datos personales, sensibles o no sensibles. Sin embargo, este tema lo abordaremos en otra ocasión con motivo de la responsabilidad penal de las personas jurídicas y el *compliance* penal.

Referencias

Díaz, E. (2006). *Teoría del delito (doctrina, jurisprudencia y casos prácticos)*. México. Straf.

Ezquiaga, F. *La argumentación interpretativa en la justicia electoral mexicana*. México. Tribunal Electoral del Poder Judicial de la Federación.

Maurach, R. (1994). *Derecho penal, parte general. Teoría general del derecho penal y estructura del hecho punible.* Trad. Jorge Bofill Genzsch y Enrique Aimone Gibson. Buenos Aires. Editorial Astrea de Alfredo y Ricardo Depalma.

Moreno, M. (2008). *Dogmática penal y política criminal*. México. Ubijus Editorial.

Roxin, C. (1997). *Derecho penal, parte general. Fundamentos. La estructura de la teoría del delito.* Trad. Diego-Manuel Luzón Peña, Miguel Díaz y García Conlledo y Javier de Vicente Remesal. Madrid. Civitas Ediciones.

Welzel, H. (1997). *Derecho penal alemán, parte general.* Trad. Juan Bustos Ramírez y Sergio Yañez Pérez. Santiago de Chile. Editorial Jurídica de Chile.

TRANSITORIOS

TRANSITORIOS

PRIMERO. El presente Decreto entrará en vigor al día siguiente al de su publicación en el *Diario Oficial de la Federación.*

SEGUNDO. El Ejecutivo Federal expedirá el Reglamento de esta Ley dentro del año siguiente a su entrada en vigor.

TERCERO. Los responsables designarán a la persona o departamento de datos personales a que se refiere el artículo 30 de la Ley y expedirán sus avisos de privacidad a los titulares de datos personales de conformidad a lo dispuesto por los artículos 16 y 17 a más tardar un año después de la entrada en vigor de la presente Ley.

CUARTO. Los titulares podrán ejercer ante los responsables sus derechos de acceso, rectificación, cancelación y oposición contemplados en el Capítulo IV de la Ley; así como dar inicio, en su caso, al procedimiento de protección de derechos establecido en el Capítulo VII de la misma, dieciocho meses después de la entrada en vigor de la Ley.

QUINTO. En cumplimiento a lo dispuesto por el artículo tercero transitorio del Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación el 30 de abril de 2009, las disposiciones locales en materia de protección de datos personales en posesión de los particulares se abrogan, y se derogan las demás disposiciones que se opongan a la presente Ley.

SEXTO. Las referencias que con anterioridad a la entrada en vigor del presente Decreto, se hacen en las leyes, tratados y acuerdos internacionales, reglamentos y demás ordenamientos al Instituto Federal de Acceso a la Información

Pública, en lo futuro se entenderán hechas al Instituto Federal de Acceso a la Información y Protección de Datos Personales.

SÉPTIMO. Las acciones que, en cumplimiento a lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, corresponda realizar al Ejecutivo Federal, se sujetarán a los presupuestos aprobados de las instituciones correspondientes y a las disposiciones de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.

OCTAVO. El Presupuesto de Egresos de la Federación para el Ejercicio Fiscal de 2011 considerará partidas suficientes para el adecuado funcionamiento del Instituto Federal de Acceso a la Información y Protección de Datos en las materias de esta Ley.

COMENTARIO

Guillermo A. Tenorio Cueto

Introducción

En ocasiones se piensa que los artículos transitorios suelen no cobrar relevancia en la integridad del cuerpo normativo, pero ello es carente de razón. Sabemos que, como ha referido el Poder Judicial:

> Los artículos transitorios de una ley, reglamento, acuerdo y, en general, de cualquier ordenamiento jurídico, forman parte de él; en ellos se fija, entre otras cuestiones, la fecha en que empezará a regir o lo atinente a su aplicación, lo cual permite que la etapa de transición entre la vigencia de un numeral o cuerpo de leyes, y el que lo deroga, reforma o adiciona, sea de tal naturaleza que no paralice el desenvolvimiento de la actividad pública del Estado, y no dé lugar a momento alguno de anarquía, por lo que la aplicación de aquéllos también es de observancia obligatoria, en términos del artículo 133 de la Constitución Política de los Estados Unidos Mexicanos.[223]

En ese sentido entendemos que el artículo transitorio evoca, en primer término, una temporalidad que permite la adecuación del sistema jurídico a partir de la norma en cuestión. Así, Huerta Ochoa refiere que "el término transitorio es elocuente, de su denominación se infiere que la función de estos artículos es, en principio, temporal y sirve para regular los procesos de cambio en el sistema

[223] Tribunales Colegiados de Circuito. Novena Época. *Semanario Judicial de la Federación* y su Gaceta. Tomo XIV. Octubre de 2001. p. 1086.

jurídico".[224] Lo anterior cobra relevancia pues sabemos también que el artículo transitorio pierde su eficacia una vez que ha logrado el cumplimiento de su mandato en el ordenamiento jurídico.[225]

A la par de lo anterior es imperante referir que existen diversos tipos de artículos transitorios tales como:

1) Los que determinan la vigencia de una norma.
2) Los que establecen la derogación de una o varias disposiciones jurídicas.
3) Los que establecen un mandato al legislador.[226]

En el caso que nos ocupa, vinculado a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, como veremos más adelante, se establecen diversas obligaciones para todos los involucrados con el cumplimiento de la norma, haciendo de capital importancia el conocimiento y estudio de los transitorios.

Análisis de contenido

Aún y cuando el tema de la protección de datos personales no era algo nuevo en nuestro sistema jurídico mexicano, lo cierto es que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares fue un parteaguas en la materia.

Sabemos que en diversas disposiciones de varias materias existían aproximaciones serias a los deberes de privacidad y confidencialidad en términos de protección de datos, e inclusive, la legislación en materia de transparencia y acceso a la información contemplaba apartados de confidencialidad de la información y de manera más puntual un incipiente deber de cuidado a los datos personales.

Sin embargo, fue hasta el 5 de julio del 2010 cuando aquella legislación vio la luz, la cual indicaba un trabajo de manera sistémica, ordenada y con una real garantía de los derechos los temas vinculados a la autodeterminación informativa. En efecto, los artículos transitorios, en términos de temporalidad, fijan la entrada en vigor de la actual Ley a partir del 6 de julio del 2010. Esto es relevante porque se da inicio a los términos que en los mismos transitorios se refieren respecto a las obligaciones que tendrán los responsables respecto

[224] Huerta, C. "Artículos transitorios y derogación". En *Boletín Mexicano de Derecho Comparado*. No. 102. IIJ-UNAM. México. Consultado en: *https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3693/4524*. Fecha de consulta: 14 de octubre de 2018.
[225] Ídem.
[226] Ídem.

al pleno ejercicio de los derechos ARCO. De igual manera, el segundo transitorio contempla la obligación del Ejecutivo Federal de la publicación del reglamento de la Ley, el cual deberá precisar los alcances de la ley respecto a su contenido.

El artículo tercero transitorio entra de lleno a la problemática central del responsable fijando un plazo concreto, tanto para la elaboración de los avisos de privacidad como para la designación, al interior, de la persona o del departamento responsable de los datos personales. El artículo transitorio otorga un año para cumplir este requisito. En el caso del aviso de privacidad, el transitorio sólo indica que el responsable deberá expedirlo en términos del contenido de la Ley. A la fecha de elaboración de este comentario han pasado ya varios años desde que entró en vigencia la Ley y todavía existen responsables que no han implementado su aviso de privacidad o no han cumplido con otras obligaciones derivadas de la Ley tal y como la designación de una persona o área de datos personales. Es imperante reconocer que el órgano garante, con infraestructura limitada para atender a la multitud de sujetos obligados, ha desarrollado acciones para el adecuado cumplimiento de la Ley. Si bien es cierto que han sido insuficientes, también hay que reconocer que han impactado de manera positiva en formar una visión adecuada de la protección de datos. Así el generador de avisos de privacidad, la disponibilidad de materiales de interés para todos los obligados y la publicación de lineamientos y modelos de sistemas de seguridad para la protección de datos han ayudado a que todos los obligados se sensibilicen sobre el tema y puedan transitar de una carencia de protección de datos a construir adecuadamente políticas y procedimientos orientados al cuidado de los mismos. De igual manera, es imperante referir que la política del órgano garante ha sido muy receptiva y colaborativa en muchos sectores que se han interesado por el cumplimiento de la Ley.

El cuarto transitorio está volcado al ejercicio de los derechos ARCO y en él encontramos el plazo de 18 meses para que los titulares puedan ejercer cualquiera de ellos en los diversos niveles de protección. Esto significa que, por un lado se le da oportunidad a los responsables de implementar políticas y procedimientos para el deber de cuidado del ejercicio de estos derechos y por otro se le conmina a la autoridad a construir el camino para que, en caso de incumplimiento, negativa o carencia de resolución por parte del responsable, el órgano garante actúe para solventar el procedimiento de protección de datos.

En efecto, la Ley en sus transitorios ordena, de manera cuidadosa, la debida construcción —en un primer momento— del documento en el que se anuncia cómo se trataran los datos. En un segundo momento precisará el área o persona encargada de implementar las políticas y procedimientos al seno de la institución y posteriormente nos habla del ejercicio de los derechos ARCO. Un responsable deberá preocuparse de detectar cómo se verifica en el seno

de su organización el tratamiento de datos para luego construir el camino por el cual se debe garantizar el ejercicio de los derechos.

Un aspecto medular de los transitorios de la Ley es lo referente a la facultad que tiene, en exclusiva, el Congreso de la Unión de legislar en materia de datos personales en posesión de los particulares contenido en el artículo 73 fracción XXIX-O. En efecto, el artículo 5 transitorio de la Ley refiere que, en virtud del otorgamiento de dicha facultad al Congreso, todas aquellas disposiciones previstas en la legislación de las entidades federativas en materia de protección de datos en posesión de los particulares deberán ser abrogadas y, desde luego, se considera de competencia federal toda aquella disposición que verse sobre la materia. Con ello, los estados no podrán legislar en materia de datos en posesión de particulares y, en consecuencia, quien velará por el cumplimiento de dicha ley será el INAI.

De igual manera, y para no generar falta de entendimiento respecto a la nomenclatura del órgano garante, el sexto transitorio refiere que se entenderá que todo lo referido en leyes, tratados y acuerdos internacionales, reglamentos y otras disposiciones al anterior Instituto Federal de Acceso a la Información (IFAI) se entenderá que hace referencia al Instituto Federal de Acceso a la información y Protección de Datos Personales (IFAIPDP). Ello cobra relevancia para no caer en la duda de un rompimiento, falta de continuidad o simplemente carencia o ausencia del órgano referido. En efecto, el transitorio otorga continuidad al órgano y provoca que todo el ordenamiento jurídico no tenga que ser reformado para la adecuación de la nueva nomenclatura entendiendo así que toda mención al anterior IFAI sigue teniendo aplicación al actual IFAIPDP. Cabe mencionar el órgano garante volvió a cambiar de nombre con motivo de la publicación de la Ley General de Transparencia y Acceso a la Información Pública de mayo de 2015 la cual le otorgó el nombre de Instituto Nacional de Acceso a la Información y Protección de Datos Personales.

Los transitorios también abordan el tema presupuestal, tanto el séptimo como el octavo refieren aspectos que obligan al poder público a realizar todas las acciones necesarias para ejecutar, de manera directa y responsable, las obligaciones que emanan de la Ley para el Ejecutivo Federal, sujetándose al presupuesto aprobado para tales efectos. De igual manera, se dota de herramientas presupuestales al anterior IFAI para que en el ejercicio fiscal 2011 se consideren las partidas necesarias para el adecuado funcionamiento de las áreas encargadas de la protección de datos.

Referencias

Huerta, C. (s.f.) "Artículos transitorios y derogación". En *Boletín Mexicano de Derecho Comparado*. No. 102. México. IIJ-UNAM. Recuperado de: *https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3693/4524* Última consulta: 14 de octubre de 2018.

Tribunales colegiados de circuito. Novena época. (2001, octubre). *Semanario Judicial de la Federación* y su Gaceta. Tomo XIV, p. 1086.

SIGLAS Y ACRÓNIMOS

AEPD	Agencia Española de Protección de Datos.
APEC	Foro de Cooperación Económica Asia Pacífico.
CIAPDP	Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.
Convenio 108	Convenio No. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
CADH	Convención Americana sobre Derechos Humanos (Pacto de San José).
CPEUM	Constitución Política de los Estados Unidos Mexicanos.
Derechos ARCO	Derechos de acceso, rectificación, cancelación y oposición.
DOF	Diario Oficial de la Federación.
IFAI	Instituto Federal de Transparencia, Acceso a la Información y Protección de Datos.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
LFTAIP	Ley Federal de Transparencia y Acceso a la Información Pública.

LFTAIPG	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
LORTAD	Ley Orgánica de Regulación y Tratamiento Automatizado de Datos.
LGTAIP	Ley General de Transparencia y Acceso a la Información Pública.
Normas Corporativas Vinculantes	(Binding Corporate Rules, BCR)
OCDE	Organización para la Cooperación y el Desarrollo Económicos.
OEA	Organización de los Estados Americanos.
ONU	Organización de las Naciones Unidas.
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de estos datos y por el que se deroga la Directiva 95/46/ CE (Reglamento General de Protección de Datos).
RIPD	Red Iberoamericana de Protección de Datos.
TJUE	Tribunal de Justicia de la Unión Europea. UE Unión Europea.

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

Edición a cargo de:
Dirección General de Comunicación Social y Difusión y la
Dirección General de Promoción y Vinculación con la Sociedad.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales