IUS REVISTA DEL INSTITUTO DE CIENCIAS JURÍDICAS DE PUEBLA, MÉXICO. ISSN 1870-2147. NUEVA ÉPOCA VOL. 12, No. 41. ENERO - JUNIO DE 2018. PP 267-291

Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento*

Protection of Personal Data in Companies Established in Mexico

Olivia Andrea Mendoza Enríquez**

RESUMEN

El desarrollo tecnológico y la economía digital, han traído entre muchas otras consecuencias, resaltar la importancia de la información en todos los sectores. Las empresas no están exentas del valor agregado que pueden dar los datos personales que forman parte de sus activos, por lo que su debido tratamiento, se ha vuelto un tema relevante en los últimos años. Factores como el uso indebido de la información o la vulneración de medidas de seguridad de la misma, ponen en riesgo la reputación de las empresas, y las podrían hacer acreedoras de sanciones, por lo que resulta necesario estudiar el tema desde una perspectiva regulatoria, que incluya: legislación, normas sectoriales y buenas prácticas.

En este sentido, las normas en el contexto nacional han contribuido a la construcción del derecho de protección de datos personales, y por ende a las obligaciones directas para el sector privado y empresas públicas, que, como parte de sus procesos, traten información.

En las siguientes líneas, el lector encontrará un análisis sobre los antecedentes del derecho de protección de datos personales, el valor económico y social de la información, el marco jurídico en materia de protección de datos personales en posesión de las empresas de servicios establecidas en México, un análisis del concepto y principios de interpretación de este derecho, y los desafíos y propuestas para implementar el cumplimiento de la Ley.

PALABRAS CLAVE

protección de datos personales, cumplimiento, principios, deberes, buenas prácticas.

ABSTRACT

Technological development and the digital economy have brought, among many other consequences, to highlight the importance of information in all sectors. Companies are not exempt from value added that personal data which forms part of its assets can give, so their due treatment has become a relevant issue in recent years. Factors such as the improper use of information or the breach of security measures, put at risk the reputation of companies, and could generate them sanctions, so it is necessary to study the issue from a regulatory perspective, which Include: legislation, sectoral regulations and good practices.

In this sense, the rules in the national context have contributed to the construction of the right to protection of personal data, and therefore to direct obligations for the private sector and public companies, which, as part of their processes, deal with information.

In the following lines, the reader will find an analysis on the background of the right to protection of personal data, the economic and social value of information, the legal framework on protection of personal data held by service companies established in Mexico, an analysis of the concept and principles of interpretation of this right, and the challenges and proposals to implement in compliance with the Law.

KEYWORDS

Protection of personal data, compliance, principles, duties, good practices

---

*Artículo recibido el 5 de julio de 2017 y aceptado el 3 de noviembre de 2017

**Centro Público de Investigación e Innovación en Tecnologías de la Información y Comunicación INFOTEC. (olivia.mendoza@infotec.mx)

SUMARIO

1. Introducción

En la sociedad de la información y el conocimiento, el manejo e intercambio de datos se ha convertido en una práctica habitual para las empresas de servicios. El uso de las tecnologías de la información y comunicación están presentes en casi todos los procesos, lo cual ha optimizado sus recursos. Sin embargo, también han propiciado una serie de desafíos en torno a la seguridad de la información, la protección de los datos personales y el cumplimiento de la regulación en la materia.

Los datos personales, en posesión de las empresas, abarcan dos vertientes: por un lado, la responsabilidad de guardar confidencialidad de los datos personales a su cargo, así como solicitar el consentimiento de los titulares, en caso de envío o cesión de información; por otro lado, el derecho que tienen los titulares de datos personales, para ejercitar sus derechos de acceso, rectificación, cancelación u oposición de datos personales (derechos ARCO).

Derivado de lo anterior, un tema recurrente que se plantea a los operadores jurídicos es el relativo al cumplimiento de la regulación en materia de protección de datos personales en posesión de las empresas. Esto atendiendo, en primer lugar, a un marco jurídico nacional que impone deberes y obligaciones en el tratamiento de datos personales y, por otro lado, el desarrollo tecnológico, que permite recabar, procesar, tratar, transmitir o remitir grandes cúmulos de información, en tiempo real y a través de técnicas de fácil acceso.

En este sentido, para dimensionar la importancia que ha cobrado el derecho de la protección de datos personales, es necesario hablar del valor económico y social de la información al interior de las organizaciones. Esto debido a que la reputación y modelo de negocio de una empresa están basados en la confianza, estándares de protección de datos personales y medidas de seguridad de la información que se implementen.

En el mismo tenor, es importante conocer la dimensión de la regulación del derecho de protección de datos personales en posesión de las empresas de servicios establecidas en México, a través del razonamiento lógico normativo que permita analizar los principios y el cumplimiento de obligaciones y deberes en la materia, atendiendo a las características propias de este derecho humano.

Los objetivos de este documento son: presentar al lector los antecedentes generales del derecho a la protección de datos personales; analizar el valor económico y social de la información de clientes y usuarios en posesión de las empresas; determinar el marco jurídico aplicable en dicha materia; conceptualizar el derecho a la protección de datos personales y especificar sus principios de interpretación; finalmente, analizar los desafíos que enfrenta el sector en el tratamiento de datos personales, así como sugerir mecanismos para el cumplimiento de la regulación en la materia.

El documento se ha realizado con base en el método deductivo, a fin de analizar el marco jurídico que puede aplicarse a la protección de datos personales de clientes y usuarios de empresas de servicios establecidas en México. Esto permite dimensionar el valor económico y social de este tipo de información, conceptualizar las implicaciones de este derecho y sus principios de interpretación, para determinar los principales desafíos y propuestas ante el cumplimiento de la legislación en la materia.

2. Valor económico y social de los datos personales

Los datos personales constituyen información dentro de las empresas. Por ello, tienen un alto valor, en cuanto a reputación en la industria y consolidación de modelos de negocio, a través de la confianza de clientes y usuarios de los servicios prestados.

Actualmente, los datos personales cuentan con un valor económico, equiparable a ciertos activos intangibles, tales como el software o el valor comercial de los nombres de dominio. Esto ha llevado a considerarlos como el petróleo de la sociedad de la información y del conocimiento.

Aunado a lo anterior, se debe decir que el valor económico otorgado a la información de las personas no radica en el dato por sí mismo, sino en el tratamiento, asociación con otros datos y utilidad que se le dé. Esto permite obtener un lucro, a través de la explotación comercial de aspectos privados, orientados al consumo, que incluso se interesan en predecir conductas y patrones de comportamiento.

En este sentido, podemos afirmar que, en la economía digital, la información se ha convertido en moneda de cambio: ha adquirido un valor elevado y permite que distintos modelos de negocio tengan su sustento en la misma.

El doctor Nelson Remolina ha estudiado la dimensión que adquirió la protección de datos personales a partir del uso de las TIC y afirma que existen jugosos modelos de negocio establecidos a partir de la información de las personas en ámbitos digitales, de modo que las empresas están interesadas en incidir en las legislaciones locales, en materia de protección de datos personales. En el mismo sentido, enfatiza la necesidad de regular la recolección internacional de los datos personales, más allá de las transferencias en el mismo contexto.[1]

Hemos visto que empresas globales, como Google o Facebook, basan su modelo de negocio en la información de las personas. Más allá de la discusión sobre si es legal y legítima esta práctica, podemos aseverar que el desarrollo tecnológico ha permitido recabar, almacenar y procesar grandes cúmulos de información en tiempo real, lo cual, le ha dado un valor agregado a la información.

En concordancia con lo antes planteado, técnicas como el *big data* permiten que las empresas basen sus decisiones en el análisis de la información, por ejemplo, el perfil de consumo mensual de sus clientes, a fin de potenciar sus ventas y tener una ventaja sobre sus competidores.

No obstante, el tratamiento y procesamiento de datos personales no siempre ha sido aparentemente inofensivo. Tal es el caso de Ashley Madison en el que, mediante una vulneración a las medidas de seguridad de la información de esta plataforma, se publicaron los nombres de usuarios adúlteros que utilizaban el servicio de citas en línea. Asimismo, el Instituto Nacional Electoral de México, a través de una nube pública, puso el padrón electoral de votantes a disposición del público en general. Estos ejemplos revelan la enorme necesidad de proteger de manera eficaz la información dentro de las empresas e instituciones.

Una vez que hemos hablado de la importancia de los datos personales y los riesgos asociados al mal uso de los mismos, es conveniente dar algunos ejemplos de los tipos de datos personales de clientes y usuarios que pueden estar en posesión de las empresas de servicios establecidas en México. Éstos pueden reflejar desde la información general, como el nombre, la edad o domicilio, hasta la información financiera de los pagos realizados o, en el peor de los casos, datos sensibles como estado de salud.

[1] Véase, Remolina Angarita, Nelson, *Recolección internacional de datos personales: un reto del mundo post-internet*, España, Agencia Española de Protección de Datos Personales, 2014.

Por ello, en la medida que los usuarios confíen en que se reguardará esa información con pleno cumplimiento a la normativa en materia de protección de datos personales, incorporando estándares de buenas prácticas, cláusulas de confidencialidad y códigos de ética, las empresas obtendrán una buena reputación en el manejo de los datos. Por ende, tales empresas no serán sujetas de sanciones impuestas, por vulneraciones al derecho de protección de datos personales.

Por otro lado, encontramos empresas que pertenecen al Estado mexicano, cuyos datos personales podrían ser desde aquellos contenidos en documentos oficiales, hasta datos personales relacionados con temas de seguridad pública, y seguridad nacional. Por tanto, se hace evidente el correcto cumplimiento de la legislación en materia de protección de datos personales.

Como se ha dicho, el valor económico de la información no puede estimarse, considerando sólo el dato personal del que se trate, pues tendría variaciones, de acuerdo a su explotación, ganancias obtenidas y tipos de negocios en los que se utilicen. No obstante, podemos proporcionar un estimado que dependerá de la situación concreta de explotación de la información.

Para tal efecto, conforme a los resultados obtenidos en el Estudio sobre el valor económico de los datos personales, de la aplicación del modelo de evaluación en 80 empresas de diversos sectores de actividad económica,[2] se concluyó que los sectores de servicios corporativos, otros servicios y servicios financieros son aquellos que obtuvieron un mayor porcentaje de sus ventas brutas por el uso de datos personales.

Por otro lado, en relación al impacto del tratamiento de los datos respecto a los gastos de operación de las empresas, los sectores de comercio al por mayor, servicios financieros y otros servicios son aquellos que asignan una mayor cantidad de recursos para el tratamiento de los datos personales.[3] Para tal efecto, se debe determinar la naturaleza de la información, la cual, atenderá al objeto y servicios que presten las empresas, el número de filiales y si comparten o reciben información con empresas terceras.

Finalmente, para el caso de México y en términos económicos, la publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados buscan consonancia para reunir estándares. Esto en busca

[2] El estudio precisa que no se trata de una muestra representativa respecto al número y distribución de empresas a nivel nacional, pero sí refleja la importancia de los datos personales para las empresas.

[3] "Estudio sobre el valor económico de los datos personales", *Asociación Mexicana de Internet*. [Consulta: 13 de mayo: 2017]. Disponible en: https://amipci.org.mx/images/valor_eco_Datospersonales_FINAL.pdf

de consolidar el intercambio comercial, por ejemplo con bloques económicos como la Unión Europea, cuya regulación es alta en la materia y establece un nivel óptimo de garantía en el derecho a la protección de datos personales, para efectos de relaciones comerciales.[4]

Derivado de lo anterior, se puede ver al derecho de protección de datos personales como un elemento primordial para incrementar exponencialmente la inversión extranjera directa.[5]

3. Marco jurídico del derecho de la protección de datos personales en México

Para comprender la importancia del derecho de protección de datos personales, debemos mencionar el antecedente internacional más importante de este derecho. Éste surge después de la Segunda Guerra Mundial, a partir de que diversos instrumentos jurídicos internacionales, invocando la dignidad humana, reconocen el derecho a la no injerencia en la vida privada de las personas, como un derecho humano.[6] Estos primeros esquemas de protección, reconocían el derecho a la vida privada y familiar como un derecho inherente a la persona, así como el respeto y la no injerencia en el domicilio y correspondencia.

Los artículos de los instrumentos internacionales referidos son: el artículo 12 de la Declaración Universal de los Derechos Humanos,[7] de 10 de diciembre de 1948; el artículo 11 de la Convención Americana de Derechos Humanos[8] (Pacto de San José de Costa Rica) de 1966; el artículo 17 del Pacto Internacional

[4] En 2017, México, a través de la Secretaría de Relaciones Exteriores, solicitó la adhesión formal al Convenio 108 del Consejo de Europa, a efectos de ser considerado como un país con niveles óptimos de protección de datos personales. Lo anterior a fin de fortalecer las relaciones comerciales de los sectores público y privado.

[5] Aunque Estados Unidos de Norteamérica no cuenta con un estatuto federal similar al Convenio 108 del Consejo de Europa, y por tanto el nivel de regulación no alcanza el estándar, el Departamento de Comercio y la Comisión Europa convinieron un marco de autorregulación. Mediante él, las empresas estadounidenses pueden obtener una certificación que permitirá que sus contrapartes europeas les transfieran datos personales sin incurrir en violaciones en la materia.

[6] El derecho de protección de datos personales, al ser reconocido como un derecho humano, adquiere las características y principios de interpretación de los derechos humanos. Por tanto, principios como la progresividad y la universalidad deberán estar presentes al momento de garantizar esta prerrogativa.

[7] "Artículo 12. 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".

[8] "Artículo 11. Protección de la Honra y de la Dignidad. 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

de Derechos Civiles y Políticos[9] de 19 de diciembre, del mismo año, 1966; el artículo 8 del Convenio Europeo de Derechos Humanos[10] de 4 de noviembre de 1950; asimismo, la Carta de los Derechos Fundamentales de la Unión Europea suscrita en Niza el 7 de diciembre de 2000.

Si bien no encontramos un reconocimiento expreso del derecho a la protección de datos personales en los instrumentos internacionales antes mencionados, sí podemos afirmar que, en el desarrollo de los derechos humanos, esta figura encuentra su antecedente más importante. Aunado a lo anterior, se debe decir que cada país ha optado por configurar el derecho a la no injerencia en la vida privada de las personas, a través de distintas figuras jurídicas. Para el caso de México, consiste en un reconocimiento constitucional del derecho de protección de datos personales, desarrollado en el marco de los postulados de la doctrina europea y los esquemas de autorregulación y sectorización del sistema anglosajón.

Dicho lo anterior, la recepción y reconocimiento del derecho de protección de datos personales en México tuvo que esperar hasta el 2002, con la Ley Federal de Acceso a la Información Pública Gubernamental, que fue el primer ordenamiento en reconocer el derecho de protección de datos personales para el ámbito público. Pero esto fue sólo una limitante al ejercicio del derecho de acceso a la información. Posteriormente, en 2009, las reformas constitucionales de los artículos 16 y 73 otorgaron el reconocimiento pleno a la protección de datos personales como un derecho fundamental y autónomo. Asimismo, estas reformas dotaron de facultades al Congreso de la Unión para legislar en la materia.

No obstante, se advertían dos grandes problemas: la legislación en materia de protección de datos personales en el sector público no garantizaba la totalidad de derechos de acceso, rectificación, cancelación y oposición,[11] y el segundo problema estaba relacionado a la falta de normativa que aplicara a la protección de datos personales en el sector privado.

---

[9] "Artículo 17. 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques".

[10] "Artículo 8. Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

[11] Los denominados derechos ARCO (acceso, rectificación, cancelación y oposición, respecto al tratamiento de datos personales) conforman el abanico de derechos comprendidos dentro del derecho de protección de datos personales, por lo que resultaba necesario garantizarlos de manera expresa para los sectores público y privado.

En este sentido, fue en 2010 cuando por primera vez se contó con disposiciones expresas que las empresas observarían para el tratamiento de datos personales en el sector privado, a través de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Finalmente, en 2017, se emitió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,[12] con la cual se terminó de armonizar la normativa en la materia en México. Así, se tienen dos legislaciones específicas que dictan obligaciones, deberes, procedimientos, sanciones y recursos en la materia, tanto para el sector público como privado.

4. Concepto y principios de interpretación del derecho de protección de datos personales

Para entender la relevancia del derecho de protección de datos personales en la sociedad de la información y del conocimiento, resulta necesario analizar los componentes del concepto, así como la clasificación de los datos personales, de conformidad con el tipo de información que reflejan.

En este sentido, el titular de los datos personales es el propio individuo y la protección de los mismos es un derecho de reciente reconocimiento en México. Los datos de un individuo son personales y éste tiene el derecho a la reserva y confidencialidad o a la cobertura mayor de la libertad de intimidad.[13]

Los datos personales refieren a la información del individuo, quien permite identificarlo a través de su descripción, origen, lugar de residencia, trayectoria académica, laboral, entre otros. Los datos personales también pueden ser sensibles, al describir aspectos sobre el individuo, como su forma de pensar, el estado de salud, las características físicas, ideología, vida sexual, entre otros.[14]

---

[12] Esta legislación es de aplicación al tratamiento de datos personales en el sector público. A diferencia de la Ley General de Transparencia y Acceso a la Información Pública de 2015, el catálogo de sujetos obligados es distinto: en materia de protección de datos personales en el sector público, se entenderán por sujetos obligados en el ámbito federal, estatal y municipal, a cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Cabe mencionar que en el caso de los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal —que, en términos del derecho de acceso a la información, sí serían sujetos obligados—, en materia de protección de datos personales, serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

[13] Gozaíni Osvaldo, Alfredo, *Derecho Procesal Constitucional hábeas data protección de datos personales*, Argentina, Rubizabal-Culzoni, pp. 113 y 114.

[14] En términos del derecho de acceso a la información, el nombre e información de contacto, de un servidor público son datos personales (porque permiten identificar a un individuo), pero no necesariamente confidenciales —como

Para Oscar R. Puccinelli, no todos los datos de carácter personal cuentan con la misma estrictez en la tutela, y refiere a la distinción que Gils Carbó hace respecto de la graduación de su protección en:

- Los datos que son de libre circulación, como los de identificación: nombre, apellido, documento de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio.
- Los de circulación restringida a un sector o actividad determinada, que son susceptibles de tratamiento en tanto se presente una causa de justificación legítima y con las limitaciones que resulten de esa especialidad.
- Los de recolección prohibida, porque afectan la intimidad personal o familiar, que son los denominados datos sensibles.[15]

Diversos instrumentos han proporcionado una definición de datos personales, entre los cuales destacan el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal, así como las directrices de la Organización para la Cooperación y el Desarrollo Económico sobre la protección de la privacidad y flujos transfronterizos de datos personales, y la Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa relativo a la protección de datos personales emitida en 1995. Esta última define como datos personales a "toda la información sobre una persona física identificada o identificable".[16]

Para el caso México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares define dato personal como cualquier información concerniente a una persona física identificada o identificable. Prevé una definición de datos personales sensibles, aquellos referentes a 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.[17]

En este sentido, se consideran datos sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro,

dicta la norma general—. Esto plantea desafíos a los operadores jurídicos, a fin de ponderar y determinar casuísticamente las posturas, al margen de dos o más derechos humanos en conflicto.

[15] Puccinelli, Oscar, Alonso, *Protección de datos de carácter personal*, Argentina, Astrea, 2004, pp. 165-169.

[16] Gómez Robledo, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*, México, Universidad Nacional Autónoma de México, pp. 16, 17 y 18.

[17] "Ley Federal de Protección de Datos Personales en Posesión de los Particulares", *Diario Oficial de la Federación*, 30 de mayo, 2016.

información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, y preferencia sexual.[18]

Son muchas las características de los datos personales, cuya importancia y significado depende de la utilización de la información que constituyan.[19] Una vez definidos los conceptos de datos personales y datos personales sensibles, el lector podrá advertir que la información que utilizan las empresas de servicios establecidas en México incluye estas dos categorías de datos, motivo por el cual, el cumplimiento de la legislación se hace primordial.

Una vez que se ha analizado el concepto del derecho a la protección de datos personales, es necesario hablar de los principios en la materia.[20] Para tal fin, resulta pertinente definir lo que se entiende por un principio en el ámbito jurídico. De acuerdo con Alexy, los principios son mandatos de optimización; es decir, son normas que ordenan la realización de algo en la medida de las posibilidades jurídicas y reales.

Dichos principios están caracterizados por el hecho de que pueden ser cumplidos en diferente grado, ya que su cumplimiento no sólo depende de las posibilidades reales, sino de las jurídicas. Esto, a su vez, está determinado por reglas y, sobre todo, por principios que juegan en sentido contrario. Por ello, es necesaria su ponderación.[21]

En este sentido, el derecho de protección de datos personales cuenta con principios enunciados en la legislación aplicable al manejo de la información, tanto para empresas públicas como privadas.

- Principio de licitud: los datos personales deberán recabarse de manera lícita, de acuerdo a las disposiciones establecidas en la legislación en materia de datos personales. La obtención de datos no puede hacerse a través de métodos engañosos o fraudulentos.[22]

[18] Mendoza Enríquez, Olivia, *Implicaciones jurídicas de la protección de datos personales en medios electrónicos de la empresa en México, Derecho del Teletrabajo*, México, Popocatépetl, 2013, p. 50.

[19] Gamboa Montejano, Claudia, "Datos personales: Estudio teórico conceptual de su regulación actual y de las iniciativas presentadas para la creación de una Ley en la materia", *Centro de Documentación, Información y Análisis de la Cámara de Diputados*, 2009, pp. 10-13. [Consulta: abril, 2017]. Disponible en: http://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-24-09.pdf

[20] Atendiendo al razonamiento lógico normativo, los principios del derecho a la protección de datos personales se aplican de acuerdo con la lógica de la preferencia y sirven para ponderar entre derechos humanos comprometidos. Por ejemplo: el principio de máxima publicidad del derecho de acceso a la información *vs.* el principio de proporcionalidad del derecho a la protección de datos personales, para determinar los límites del ejercicio derechos humanos.

[21] Alexy, Robert, *Teoría de los derechos fundamentales*, Madrid, cec, 1993, pp. 458 y 459.

[22] Artículo 7 de la lfpdppp y artículo 17 de la lgpdppso.

- Principio de finalidad: todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera, o en el caso de empresas privadas, que el tratamiento de datos personales se limite al cumplimiento de las finalidades previstas en el aviso de privacidad.[23]
- Principio de lealtad: el responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos. Tendrá que privilegiar la protección de los intereses del titular de los datos personales y la expectativa razonable de privacidad, y velará por el cumplimiento de los principios de protección de datos personales, establecidos en la legislación, debiendo adoptar medidas necesarias para su aplicación.[24]
- Principio de consentimiento: todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas en la legislación en la materia. 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 manifiesta su oposición. Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo excepciones de ley.[25]
- Principio de calidad: el responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados según los fines para los cuales fueron recabados. Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.[26]
- Principio de proporcionalidad: el tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. El responsable sólo deberá tratar

[23] Artículos 12 de la LFPDPPP y 18 de la LGPDPPSO.
[24] Artículos 19 de la LGPDPPSO.
[25] Artículo 8 de la LFPDPPP y artículo 22 de LGPDPPSO.
[26] Artículo 11 LFPDPPP y artículo 23 de la LGPDPPSO.

los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.[27]

- Principio de información: el responsable tendrá la obligación de informar a los titulares de los datos la información que se recabe de ellos y su finalidad. El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.[28] Asimismo, se refiere a la potestad que otorga la Ley, de conocer previamente las características esenciales del tratamiento a que serán sometidos los datos personales que se proporcionen a un ente privado o empresa. El aviso de privacidad deberá ser redactado en un lenguaje claro y comprensible.
- Principio de responsabilidad: 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.[29]

Aunados a los principios anteriores, existen deberes en materia de protección de datos personales. Éstos consisten en guardar confidencialidad de la información y establecer medidas de seguridad de la información, adecuadas e iguales a las que las empresas utilizan para guardar su propia información.

Finalmente, en relación con los principios del derecho a la protección de datos personales, las leyes específicas en la materia no reconocen de manera expresa el principio del interés superior del menor. Sin embargo, su aplicación es de carácter transversal, no sólo al derecho de protección de datos personales, sino a la efectiva tutela de los derechos humanos. Este principio podrá invocarse cuando se trata de la protección de datos de niños, niñas o adolescentes, lo cual significa la protección más amplia a éstos, de acuerdo con la legislación en la materia.[30]

[27] Artículo13 de la LFPDPPP y 25 LGPDPPSO.

[28] Artículos 15 de la LFPDPPP y 26 LGPDPPSO.

[29] Artículo 14 de la LFPDPPP.

[30] Artículo 2 de la Ley General de los Derechos de los Niños, Niñas y Adolescentes: "Para garantizar la protección de los derechos de niñas, niños y adolescentes, las autoridades realizarán las acciones y tomarán medidas, de conformidad con los principios establecidos en la presente Ley. [...] El interés superior de la niñez deberá ser considerado de manera primordial en la toma de decisiones sobre una cuestión debatida que involucre niñas, niños y adolescentes. Cuando se presenten diferentes interpretaciones, se elegirá la que satisfaga de manera más efectiva este principio rector. Cuando se tome una decisión que afecte a niñas, niños o adolescentes, en lo individual o colectivo, se deberán evaluar y ponderar las posibles repercusiones a fin de salvaguardar su interés superior y sus garantías procesales".

5. Desafíos y cumplimiento de la regulación en materia de datos personales en las empresas en México

En las siguientes líneas, de manera general, se enuncian los principales desafíos que enfrentan las empresas de servicios establecidas en México, en relación a la protección de datos personales, a fin de cumplir con las obligaciones y responsabilidades establecidas en la legislación en la materia. Asimismo, se presentan algunas soluciones y esquemas generales de cumplimiento, en razón de lo establecido por el marco jurídico aplicable.

Es importante destacar que, atendiendo a la diversidad de datos personales que tratan las empresas establecidas en México, las siguientes líneas se centrarán en aquellos desafíos y esquemas de cumplimiento del marco de protección de datos personales de empresas de servicios.[31]

El Estudio de protección de datos personales entre usuarios y empresas de 2012, evaluó tanto a internautas mexicanos como empresas en territorio nacional. Proporciona una noción de los problemas y retos en el cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y nos permite establecer los principales desafíos en torno al mismo.

En este sentido, 44 % de las empresas evaluadas no poseen el conocimiento necesario sobre la LFPDPPP. En relación con el ejercicio de derechos ARCO, 50 % de empresas evaluadas no tiene el conocimiento necesario para su atención y, por lo tanto, podrían ser acreedoras a una sanción por el incumplimiento a las disposiciones de la LFPDPPP.

En el mismo tenor, 30 % de las empresas no conocen las acciones que han emprendido para realizar el cumplimiento de la citada ley y, del resto de empresas, 48 % han emprendido acciones de capacitación de personal dentro de su organización. Mientras 20% han contratado a una empresa legal especializada en esos temas, sólo 6% ha contratado a una persona especializada en la ley.

No obstante, 69 % de las empresas consideran una ventaja comercial informar sobre el tratamiento de los datos personales de sus clientes o usuarios. Con ello, se genera confianza y se distinguen de las demás empresas que ofrecen servicios similares. Sin embargo, 50 % de las empresas considera que el cumplimiento de la LFPDPPP genera gastos adicionales.

[31] Las empresas, de acuerdo con su actividad o giro, se pueden clasificar en empresas de servicio y son aquellas que brindan un servicio a la comunidad, las cuales pueden tener o no fines lucrativos. Véase HERNÁNDEZ Y RODRÍGUEZ, SERGIO, *Fundamentos de administración*, México, McGraw Hill, 2000

Es importante destacar que 74 % de empresas consideran que no se ha difundido apropiadamente el impacto de la ley en las empresas establecidas en México.[32] Por lo anterior, se advierte que existe poca cultura de la protección de datos personales en posesión de las empresas establecidas en México, pues la legislación existente, en algunos puntos, se considera sobrerreguladora y obstáculo de la innovación. En la mayoría de los casos, no se vislumbra como un elemento generador de confianza para los clientes y usuarios de servicios ofrecidos, ni motivo de inversión y consolidación de intercambio comercial.

Para entender la dimensión que tiene el cumplimiento de disposiciones en materia de protección de datos personales en posesión de empresas de servicios establecidas en México, debemos decir que el modelo mexicano es un modelo híbrido, resultado de la incorporación de la visión europea en la protección de este derecho y de algunos elementos del derecho anglosajón. Esto toda vez que la protección de datos personales en nuestro país se eleva al valor de un derecho humano, pero también reconoce esquemas de autorregulación y legislación sectorial, por lo cual se hace más complejo el cumplimiento en la materia.

Las disposiciones en materia de protección de datos personales se encuentran señaladas principalmente en dos ordenamientos: el primero, para el sector privado (LFPDPPP) y de aplicación federal; el segundo, para el sector público (LGPDPPSO) y de aplicación en los tres órdenes de gobierno (federal, estatal y municipal). No obstante, existen excepciones sectoriales para la aplicación de estas dos leyes, atendiendo, por ejemplo, a si los datos son de carácter fiscal, financiero o clínicos.

Lo anterior se traduce en que los operadores jurídicos deberán conocer un cúmulo de legislación, que no refiere únicamente a la materia en específico, sino a documentos de interpretación, de orientación o vinculatorios. Éstos son emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Inai), órgano garante de la protección de datos personales en el país. Ejemplo de estos documentos son, por ejemplo, la Guía para el borrado seguro de datos personales, las Guías de atención a solicitudes de derechos ARCO, así como los criterios y resoluciones emitidas por este instituto.

Las siguientes líneas abordan los aspectos generales de cumplimiento de las principales disposiciones específicas en materia de protección de datos personales en posesión de empresas de servicios establecidas en México.

---

[32] "Estudio de Protección de Datos Personales entre Usuarios y Empresas", *Asociación Mexicana de Internet*. Disponible en: https://www.asociaciondeinternet.mx/es/component/remository/Proteccion-de-Datos-Personales/Estudio-de-Proteccion-de-Datos-Personales-entre-Usuarios-y-Empresas/lang,es-es/?Itemid=

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

La LFPDPPP tiene por objeto proteger los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado. Esto con el fin de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Asimismo, este ordenamiento reconoce los principios de interpretación reconocidos como estándar internacional en la materia.

En lo que respecta a los sujetos regulados por esta ley, son todas aquellas personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, exceptuando a las sociedades de información crediticia[33] y las personas que traten datos para su uso personal.

Cabe resaltar que, ajustándose a lo que marca la LFPDPPP, los poseedores de los datos deben dar a conocer a los titulares, la información que de ellos se recaba y los fines para los cuales serán utilizados sus datos, a través del aviso de privacidad.

De igual manera, la LFPDPPP estipula obligaciones para los particulares que lleven a cabo el tratamiento de datos personales, respecto a la seguridad administrativa, técnica y física que permita proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. En caso de existir alguna vulneración de seguridad, el responsable deberá informar inmediatamente al titular, a fin de que éste pueda emprender acciones que ayuden a la defensa de su derechos.

La ley, como se constata en los artículos 19 y 20, considera mecanismos que, frente al desarrollo de las nuevas tecnologías de la información y de las vulnerabilidades implícitas en ellas, permitan tomar medidas operativas, tanto al responsable como al titular de los datos.

Cabe señalar también lo estipulado por la LFPDPPP respecto a las transferencias nacionales o internacionales de datos, las cuales aumentarán en tanto los sectores público y privado comiencen a adoptar esquemas de cómputo en la nube. Recordemos que, en la mayoría de los casos, los centros de datos se encuentran fuera del país.[34] Estas transferencias, de acuerdo a la LFPDPPP, sólo

[33] La Ley de Instituciones de Crédito dicta las disposiciones en relación con los datos financieros.

[34] Uno de los pocos centros de datos del sector público en México que tiene certificación TIER III emitida por el *Uptime Institute* se encuentra en el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación Infotec (perteneciente a la red de Centros Públicos del Consejo Nacional de Ciencia y Tecnología Conacyt). Esto significa que prestan servicios de almacenamiento con un nivel óptimo de disponibilidad, balanceo de cargas, respaldo de energía y seguridad para hacer frente a los recursos de información, cuya jurisdicción aplicable sería la mexicana, en caso de un conflicto.

podrán realizarse en tanto el titular otorgue su consentimiento y, tratándose del responsable, éste deberá comunicar al receptor, el aviso de privacidad e informar las finalidades a las que el titular sujetó su tratamiento.

En todo tratamiento de datos, existe una expectativa razonable de privacidad. Por ello, se presume que, tratándose de una transferencia de datos internacional, el titular de los datos confía en que su información será tratada conforme al aviso de privacidad, pues éste deberá asumir las mismas obligaciones que corresponden al responsable transferente.

El régimen nacional de transferencias, por su parte, sigue un camino similar al régimen internacional de transferencias. Así, se exige que el receptor trate los datos conforme al aviso de privacidad, el cual deberá ser previamente comunicado por el transferente. En lo referente a infracciones, la LFPDPPP contempla en su capítulo 10, De las infracciones y sanciones, un listado de acciones que serán motivo de sanción.

Las penas, para quienes estén en los supuestos señalados, consisten en una multa de 100 a 320 000[35] días de salario mínimo vigente en la Ciudad de México, con la posibilidad de que la pena se duplique si las infracciones son cometidas en el tratamiento de datos sensibles.[36]

5.2. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Después de buscar el punto medio entre su debida protección y un bajo impacto en los costos de cumplimiento para los sujetos regulados por la LFPDPPP, se publicó el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, con fecha 21 de diciembre de 2011. Esto con el fin de completar la estructura jurídica relacionada con la protección de datos personales.

En su capítulo 1, este reglamento clarifica el ámbito de aplicación, territorial y objetivo, de la norma y establece supuestos en los cuales la norma es aplicable. El reglamento, asimismo, define los derechos ARCO y también conceptos relacionados con los nuevos entornos generados por las tecnologías de la información y la comunicación.

[35] Uno de los casos paradigmáticos en la materia lo constituye la multa impuesta a Banamex por el incumplimiento de las disposiciones en materia de protección de datos personales.

[36] Al cierre de este trabajo, el legislativo no ha armonizado las multas previstas en la ley con la referencia del valor de la unidad de medida y actualización.

En el capítulo 2 del reglamento se señala el alcance de los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, los cuales deberán ser observados por los responsables de datos personales. Su capítulo 3 engloba una serie de pautas para el sujeto obligado respecto a la seguridad de la información. Asimismo, establece los factores aplicables a los datos personales que se deberán tener en cuenta para determinar las medidas de seguridad. Respecto a las transferencias de datos personales, se encuentran sujetas al consentimiento de su titular, salvo las excepciones enmarcadas por el artículo 37 de la LFPDPPP.

Considerando el avance de los sistemas automatizados de tratamiento de datos, el reglamento contiene, en su artículo 112, la obligación del responsable de informar al titular el tratamiento de sus datos personales, sin la intervención o valoración humana. Este artículo resulta aplicable si los datos son tratados por los sistemas automatizados de los particulares que radican en el territorio nacional, o que, encontrándose fuera del territorio, hayan sido terceros receptores de datos. Por tanto, quedarían sujetos a lo enmarcado por el artículo 36 de la LFPDPPP: asumirán las mismas obligaciones correspondientes al responsable que transfirió los datos.

El artículo 112 del reglamento, sin embargo, carece de fuerza ante la recolección de datos que hacen en internet las empresas privadas con establecimientos en otros países. Es así como, frente al avance de las nuevas tecnologías y de las nuevas maneras de procesar, analizar, almacenar y utilizar los datos personales —pensemos, por ejemplo, en el *big data*—, el reglamento se vuelve inoperante.

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

La Ley General de Protección de Datos en Posesión de Sujetos Obligados es el ordenamiento jurídico más reciente en materia de protección de datos personales, pues fue publicado el 26 de enero de 2017. Tiene vital importancia en la protección de la información porque, por primera vez, se cuenta con una legislación acorde a las características del sector público.

Este ordenamiento resulta particular porque su ámbito de aplicación abarca los tres niveles de gobierno. Así, contempla un catálogo de sujetos obligados, dentro de los cuales se encuentra cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos y, para fines de este documento, las empresas del Estado mexicano.

Esta Ley establece las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados. Entre otros objetivos, busca establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos; garantizar la observancia de los principios de protección de datos personales.

Sobre todo, busca proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de regular su debido tratamiento; garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales, y establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en esta ordenamiento, así como regular los medios de impugnación.

Los elementos más relevantes de este ordenamiento refieren al reconocimiento pleno de la totalidad de derechos ARCO (acceso, rectificación, cancelación y oposición, respecto al tratamiento de datos personales). También, por primera vez, se habla del concepto portabilidad de los datos. Éste se refiere a que, cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado, el cual le permita seguir utilizándolos.

Por otro lado, se hace una diferencia entre los conceptos de responsable y encargado, a fin de definir las facultades y responsabilidades respecto al tratamiento de datos personales. Además, cubre la necesidad de formalizar esta relación mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.

Existen disposiciones relativas a las transferencias de datos personales, reconociendo que pueden ser nacionales e internacionales y manifestando que se encuentran sujetas al consentimiento del titular de los datos personales.[37]

[37] Las únicas excepciones del consentimiento respecto a transferir datos personales son cuando una ley así lo disponga, cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales; cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente; para el reco-

En relación con las acciones preventivas, como parte de las buenas prácticas, el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas. Esto para elevar el nivel de protección de los datos personales; armonizar el tratamiento de datos personales en un sector específico; facilitar el ejercicio de los derechos ARCO por parte de los titulares; facilitar las transferencias de datos personales; complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales. Por último, el responsable podrá demostrar, ante el órgano garante de la protección de datos personales, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.

A manera de conclusión, los elementos más relevantes de cumplimiento de la normativa en materia de protección de datos personales en posesión en empresas de servicios establecidas en México son:

- Elaboración de avisos de privacidad, cumpliendo con los requisitos de la ley, y redactados con un lenguaje claro y sencillo, que permita entender a los clientes, los alcances del consentimiento que está otorgando, respecto al tratamiento de datos sus personales.
- Una vez que el dato ha sido recabado, garantizar que, durante el ciclo del mismo, se cumplan con los requerimientos señalados en la normativa en la materia y que el tratamiento del dato se haga conforme los principios del derecho a la protección de datos personales.
- Garantizar procedimientos efectivos de ejercicio de derechos de acceso, rectificación, cancelación y oposición (ARCO), así como de portabilidad de los datos.
- Establecer cláusulas de confidencialidad de la información, en los contratos que se celebren para establecer relaciones laborales, para que, de manera expresa, los trabajadores no puedan sustraer, utilizar o transmitir datos personales o información de la empresa.

nocimiento o defensa de derechos del titular ante autoridad competente; cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria; cuando los datos personales figuren en fuentes de acceso público; cuando los datos personales se sometan a un procedimiento previo de disociación, o cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

- Establecer mecanismos técnicos que limiten el acceso a los datos personales, de acuerdo a las funciones de los puestos de trabajo, así como sistemas de autenticación y esquemas de privacidad por diseño.
- Capacitar al personal que lleve a cabo tratamiento de datos personales, a fin de sensibilizarlo en las implicaciones que podría tener hacer un mal uso de la información y de que conozca la regulación jurídica en la materia.
- Verificar las medidas físicas y digitales de seguridad de la información al interior de la empresa, así como las políticas de ciberseguridad instrumentadas a la luz de la normativa en materia de protección de datos personales.
- Revisar que, en la contratación de servicios de almacenamiento de información —como el cómputo en la nube— se garantice, por lo menos: la obligación de dar aviso en caso de cualquier vulneración a las medidas de seguridad de la plataforma electrónica, la portabilidad y destrucción de los datos al término del contrato, mecanismos alternativos de resolución de controversias como la mediación electrónica, la reputación y políticas de transparencia de la empresa a contratar, que se privilegie la jurisdicción nacional en la prestación del servicio, las medidas compensatorias en caso de vulneraciones y mal uso de la información, así como evitar contratos de adhesión que no atiendan a las características de los datos a almacenar, de acuerdo al tipo de información, servicio y empresa.
- En caso de que sea necesario, contar con un Encargado de los datos personales, se deberá verificar que, en la relación contractual entre Responsable y Encargado, se garantice por lo menos: que el tratamiento de datos personales se hará conforme a las instrucciones del responsable, que no se traten datos personales para finalidades distintas a las instruidas por el Responsable, que se implementen las medidas de seguridad conforme a los instrumentos jurídicos aplicables, que se informe al Responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones, que se guarde confidencialidad respecto de los datos personales tratados, que se suprima o devuelvan los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, (siempre y cuando no exista una previsión legal que exija la conservación de los datos personales), y que se abstenga de transferir los datos personales salvo en el caso de que el Responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

- Aunado al cumplimiento de la normativa en materia de protección de datos personales, existe la posibilidad de que un organismo certificador avale que las empresas cumplan con la efectiva protección de los datos personales en su poder.
- En este sentido, el artículo 83 del Reglamento de la LFPDPPP prevé un elemento que podrán incorporar los esquemas de autorregulación, al señalar que, "los esquemas de autorregulación vinculante podrán incluir la certificación de los responsables en materia de protección de datos personales. En caso de que el responsable decida someterse a un procedimiento de certificación, ésta deberá ser otorgada por una persona física o moral certificadora ajena al responsable, de conformidad con los criterios que para tal fin establezcan los parámetros a los que refiere el artículo 43, fracción V de la ley".
- Asimismo, el artículo 85 del citado ordenamiento señala que los parámetros de los esquemas de autorregulación "contendrán los mecanismos para acreditar y revocar a las personas físicas certificadoras, así como sus funciones; los criterios generales para otorgar certificados en materia de protección de datos personales".[38]
- Derivado de lo anterior, la normalización y certificación electrónica (NYCE) es el organismo que el INAI y la Secretaría de Economía han acreditado para avalar que las empresas cumplan con la normativa en materia de protección de datos personales.

En concreto, se propone dimensionar la privacidad y la protección de datos personales como una condición indispensable para el desarrollo económico, a través de las siguientes acciones:

- Promover una cultura de la protección de datos personales en posesión de las empresas de servicios establecidas en México, a fin de sensibilizar a todos los integrantes de las organizaciones, del daño irreparable que puede ocasionar el incumplimiento de las disposiciones en la materia.
- Establecer campañas permanentes de capacitación, a fin de dar a conocer las obligaciones en lo particular, que deben ser observadas por los integrantes de las empresas, de acuerdo a la naturaleza de la información que tratan.

[38] "Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI", *Secretaría de Economía*. [Consultado: 30 de abril, 2017]. Disponible en: https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_04.pdf

- Elaborar un inventario de los datos personales que tienen en su poder, a fin determinar si se tratan datos personales, datos personales sensibles, o ambos.
- Con base en dicho inventario, elaborar una metodología de cumplimiento a la LFPDPPP. Deberá incluir un apartado de auditoría externa que observe el cumplimiento de los deberes y responsabilidades en la materia.
- Establecer como parte de los esquemas de buenas prácticas, incentivos al adecuado tratamiento de datos personales, conforme a las disposiciones de ley.
- Dar a conocer las sanciones a las cuales se puede ser acreedor en caso de incumplimiento de los deberes, responsabilidades y principios de la LFPDPPP.
- Encontrar en la efectiva protección de datos personales en posesión de las empresas establecidas en México una oportunidad para generar confianza entre los clientes y sus usuarios, y por lo tanto una forma de consolidación de los modelos de negocio.

Entender la implementación de las medidas de seguridad de la información bajo un enfoque multidisciplinario en el cual abogados e ingenieros instrumenten el efectivo cumplimiento de las disposiciones de la Ley [39].

Apostar por los esquemas de autorregulación para generar buenas prácticas en los modelos de protección al interior de las organizaciones y compartir las experiencias entre empresas del mismo sector.

6. Conclusiones

El derecho a la no injerencia en la vida privada de las personas es un derecho humano reconocido desde la Declaración Universal de los Derechos Humanos de 1948. Sin embargo, en el caso de México, el reconocimiento expreso del régimen de protección de datos personales en posesión de las empresas se hizo hasta 2010, lo cual ha propiciado un desfase de la regulación en la materia, en contraste con otros países.

[39] En relación con el principio de responsabilidad y de las disposiciones de la LEFPDPPP, en el tratamiento que lleven a cabo las empresas respecto a los datos personales de sus clientes o usuario se debe procurar el mismo cuidado que los recursos financieros de la empresa. En el mismo tema, la falta de políticas de ciberseguridad propician que las medidas y protocolos de seguridad de la información no sean adecuados, atendiendo al tipo de información y datos de que se trata.

Los datos personales tienen un alto valor económico y social. En su protección se encuentra una oportunidad para generar confianza entre los clientes y usuarios de servicios, para así consolidar los modelos de negocio.

Si bien el impulso de la regulación en materia de protección de datos personales para empresas establecidas en México atiende a la garantía de un derecho humano, también encuentra su origen en aspectos económicos a nivel internacional. Alcanzar estándares de niveles adecuados de protección de la información ha sido una condicionante para que el país se pueda declarar seguro en el intercambio comercial.

A pesar de que el marco jurídico en materia de protección de datos personales en posesión de las empresas de servicio establecidas en México recoge estándares internacionales y proporciona garantías para la efectiva tutela de este derecho, el cumplimiento de las disposiciones enfrentan grandes desafíos. Ejemplo de ello es el desconocimiento de las implicaciones legales del tratamiento de la información, la falta de ética en dicho tratamiento, la desensibilización respecto a las repercusiones del mal uso de la información y el desconocimiento de los mecanismos legales para exigir este derecho.

En México, el derecho de protección de datos personales es un derecho humano que se reconoce a nivel constitucional, en dos leyes específicas en la materia (LFPDPPP y LGPDPPSO). Asimismo, reconoce legislación sectorial, que dicta disposiciones específicas, por ejemplo, cuando se trata de datos fiscales, financieros o de salud. Esto es la causa de que los operadores jurídicos necesiten conocer un cúmulo de documentos, algunos no vinculatorios, a fin de poder cumplir con todas las exigencias de salvaguarda de la información.

Los principios del derecho de protección de datos personales ayudan a su interpretación, sobre todo frente a colisión de derechos humanos como el de acceso a la información y el de protección de datos personales. En este sentido, a pesar de no estar expresamente reconocido en la ley en la materia, se deberá atender al principio del interés superior del menor como eje transversal en la garantía de los datos personales de niñas, niños y adolescentes.

El cumplimiento de la legislación en materia de protección de datos personales en posesión de empresas de servicios establecidas en México es mínimo, como consecuencia del desconocimiento de la ley. Se advierte que los esquemas de buenas prácticas y el uso ético de la información podrían traer como resultado la efectiva garantía del derecho a la protección de datos personales, incluso de mejor manera que la ley por sí misma.

Bibliografía

Alexy, Robert, *Teoría de los derechos fundamentales*, Madrid, cec, 1993.

"Carta de los Derechos Fundamentales de la Unión Europea", *Parlamento Europeo*. Disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf

"Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica)", *Organización de los Estados Americanos*. Disponible en: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf

"Convenio Europeo de Derechos Humanos", *European Court of Human Rights*. Disponible en: http://www.echr.coe.int/Documents/Convention_SPA.pdf

"Declaración Universal de los Derechos Humanos", *Naciones Unidas, Derechos Humanos*. Disponible en: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

"Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI", *Secretaría de Economía*. [Consultado: 30 de abril, 2017]. Disponible en: https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_04.pdf

"Estudio de Protección de Datos Personales entre Usuarios y Empresas", *Asociación Mexicana de Internet*. Disponible en: https://www.asociaciondeinternet.mx/es/component/remository/Proteccion-de-Datos-Personales/Estudio-de-Proteccion-de-Datos-Personales-entre-Usuarios-y-Empresas/lang,es-es/?Itemid=

"Estudio sobre el valor económico de los datos personales", *Asociación Mexicana de Internet*. [Consulta: 13 de mayo: 2017]. Disponible en: https://amipci.org.mx/images/valor_eco_Datospersonales_FINAL.pdf

Gamboa Montejano, Claudia, "Datos personales: Estudio teórico conceptual de su regulación actual y de las iniciativas presentadas para la creación de una Ley en la materia", *Centro de Documentación, Información y Análisis de la Cámara de Diputados*, 2009. [Consulta: abril, 2017]. Disponible en: http://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-24-09.pdf

Gómez Robledo, Alonso *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*, México, Universidad Nacional Autónoma de México.

Gozaíni Osvaldo, Alfredo, *Derecho Procesal Constitucional hábeas data protección de datos personales*, Argentina, Rubizabal-Culzoni.

Hernández y Rodríguez, Sergio, *Fundamentos de administración*, México, McGraw Hill, 2000.

Mendoza Enríquez, Olivia, *Implicaciones jurídicas de la protección de datos personales en medios electrónicos de la empresa en México, Derecho del Teletrabajo*, México, Popocatépetl, 2013.

"Pacto Internacional de Derechos Civiles y Políticos", *Naciones Unidas, Derechos Humanos*. Disponible en: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Puccinelli, Oscar, *Protección de datos de carácter personal*, Argentina, Astrea, 2004.

Remolina Angarita, Nelson, *Recolección internacional de datos personales: un reto del mundo post-internet*, España, Agencia Española de Protección de Datos Personales, 2014.