derecom

ISSN: 1988-2629. Nº. 26. Nueva Época. Marzo 2019-Septiembre 2019

Cómo citar este texto:
Rosa María de la Torre Torres y Brenda Yessenia Olalde Vázquez. (2019). La aplicación extraterritorial del Reglamento General de Protección de Datos (RGPD) de la Unión Europea: implicaciones en México. *Derecom*, 26, 99-114. http://www.derecom.com/derecom/

LA APLICACIÓN EXTRATERRITORIAL DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) DE LA UNIÓN EUROPEA: IMPLICACIONES EN MÉXICO

EXTRATERRITORIAL ENFORCEMENT OF THE EUROPEAN UNION GENERAL REGULATION ON DATA PROTECTION (GDPR): CONSEQUENCES FOR MEXICO

© Rosa María de la Torre Torres
Universidad Michoacana de San Nicolás de Hidalgo (México)
rosdelatorre@gmail.com

©Brenda Yessenia Olalde Vázquez
Universidad Michoacana de San Nicolás de Hidalgo (México)
iuslitis@gmail.com

Resumen

El 25 de mayo de 2018 entró en vigor al Reglamento General de Protección de Datos, relativo a la Protección de los Datos Personales de las Personas Físicas y a la Libre Circulación de Datos. Este ordenamiento comunitario tiene implicaciones allende las fronteras de la Unión.

El objetivo de este trabajo es analizar el efecto de aplicación extraterritorial de este nuevo reglamento en el espacio jurídico de la protección de datos en México.

Los considerados y artículos del RGPD relativos a la aplicación extraterritorial del mismo son de especial interés porque contribuyen a diluir las fronteras jurídicas que, hasta hace poco, obstaculizaban la efectiva protección de datos personales en los ordenamientos estatales.

Son tres los aspectos de especial relevancia que aporta esta normativa en materia de protección de datos: en lo relativo a las actividades de tratamiento, que estén relacionadas con la oferta de bienes o servicios a interesados en la UE, las actividades de tratamiento de datos personales por parte de Responsables y/o Encargados del tratamiento no establecidos en la UE y tratamientos de datos personales realizados por Responsables a los que, no estando establecidos en la UE, les sea aplicable el Derecho de un Estado Miembro por aplicación de Derecho Internacional Público.

Recibido: 28/01/2019 Revisado: 11/03/2019
Aceptado: 12/03/2019 Publicado: 15/03/2019

La regulación analizada establece nuevos e interesantes parámetros en materia de aplicación territorial, implicando a empresas y sujetos que anteriormente no se verían afectados por la misma.

Summary

On May the 25th, 2018 came into force the EU General Data Protection Regulation (GDPR), relating to the Protection of Personal Data of Persons and the Free Movement of Data. This European Union Regulation has implications beyond the borders of the very same EU.

The aim of this paper is to analyze the effect of the extraterritorial application of the new Regulation of the EU, in the Mexican legal space of data protection.

The recitals and articles of the GDPR related to the extraterritorial application of this regulation are of special interest as they help to blur the juridical borders that, until recently, hindered the effective protection of personal data in the state legislations.

There are three aspects of main relevance that this regulation provides for in terms of data protection: concerning the data processing activities related to the supply of goods or services to interested parties in the EU, the activities of processing personal data by a controller or a processor not established in the EU and the processing of personal data made by controllers not settled in the EU and to whom the Law of a Member State is applicable due to International Public Law.

The analyzed Regulation here sets new interesting parameters in terms of territorial application, involving companies and individuals that previously would not be affected by it.

Palabras clave: Méjico. Unión Europea. Protección Datos. Extraterritorialidad.

Keywords: Mexico. European Union. Data protection. Extraterritoriality.

1. Introducción.

El desarrollo tecnológico de los últimos treinta años ha tenido un impacto real en la calidad de vida de las personas. Se han generado instrumentos y herramientas que facilitan las actividades cotidianas tanto de personas físicas como de empresas e instituciones.

El Internet es el mejor ejemplo de una herramienta poderosa por su nivel de penetración entre usuarios de muy diverso perfil. La denominada Red de Redes está presente a lo largo y ancho de nuestro planeta, incidiendo en la vida social, cultural, económica y política de los seres humanos.

2. La protección de datos personales, un reto global.

Esta permeabilidad y su naturaleza global han tenido como consecuencia que la regulación de las actividades que se desarrollan en la Red, las interacciones sociales y comerciales, sea muy compleja y represente un reto a las instituciones jurídicas tradicionales.

Hablar de regulación en materia de Internet es hablar del conjunto de esfuerzos nacionales e internacionales para responder a retos globales. Si bien en un inicio los Estados intentaron, desde sus legislaciones nacionales, dar cabal respuesta a la problemática derivada del uso del Internet (posibles violaciones al derecho a la intimidad, la propia imagen, protección de datos personales, atentados contra la seguridad nacional, entre otros varios) muy pronto se dieron cuenta de que se requiere la cooperación entre Estados y entre Estados y organismos supranacionales para dar una respuesta efectiva a estos desafíos.

Los datos personales son aquella información del individuo que permite establecer un lazo de identificación mediante la descripción de elementos que determina un perfil específico tales como su lugar de residencia, su origen, su trayectoria académica y laboral. Además de los anteriores, también forman parte de los datos personales aquéllos de carácter sensible como el estado de salud, las preferencias sexuales, las filiaciones ideológicas, las creencias religiosas, entre otras que se consideran datos personalísimos y sensibles debido a que dan cuenta de la esfera más íntima del ser humano.

Así, encontramos que los datos personales, por su naturaleza y contenido, pueden ser clasificados acorde con el nivel de protección que requieren:

a. 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.

b. 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.

c. Los de recolección prohibida, porque afectan la intimidad personal o familiar, que son los denominados datos sensibles.

La definición de datos personales se encuentra contenida en diversas fuentes.

En Europa, pionera en el tema, 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 Privacidad y Flujos Transfronterizos de Datos Personales, así como la Directiva 95/46/CE y ahora el Reglamento General para la Protección de Datos de la Unión Europea (RGDP) definen claramente lo que debe entenderse por datos personales y su clasificación.

En el artículo 4º del RGPD se define a los datos personales como:

> *toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o*

> *uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*.[1]

Por su parte, el Convenio 108 define los datos personales de la siguiente manera en su artículo 2º. Apartado A: *significa cualquier información relativa a una persona física identificada o identificable*.[2]

Para el caso de 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.

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.

En este sentido, se consideran datos 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 y preferencia sexual.

La mayoría de los elementos normativos coincide en definir y clasificar la información que se considera como datos personales, cuya importancia dependerá en gran medida de la utilización que se dé a los mismos. Así, podemos observar que las empresas que prestan servicios u ofrecen productos manejan datos personales tanto generales como sensibles, los cuales son, en la mayoría de los casos, proporcionados voluntariamente por el usuario o consumidor. Por ello, el cumplimiento de los principios y la normativa vigente en la materia es ineludible para dichas empresas o instituciones.

3. Estado de la cuestión.

El 6 de abril de 2016, fue acordado por la Unión Europea un conjunto de disposiciones en materia de protección de datos que incluye el Reglamento General de Protección de Datos (RGPD), el cual sustituye a la Directiva 95/46/CE sobre Protección de Datos que tenía una vigencia de más de veinte años. Este conjunto de normas pretende dar mayor garantía a la protección de datos como un derecho fundamental en toda la Unión Europea y a sus ciudadanos y residentes más allá de sus fronteras.

Aunque el nuevo Reglamento tiene su origen en normativa previa, requirió ajustes considerables en varios aspectos, por lo que se dio un plazo de dos años, hasta el 25 de mayo de 2018, a fin de que los Estados miembros y las partes interesadas pudieran prepararse para la implementación del nuevo marco jurídico.

Con la entrada en plena vigencia del Reglamento, el régimen de protección de datos de la Unión Europea alcanza incluso a compañías extranjeras, que no estén establecidas dentro

del territorio de la Unión, que manejen datos de personas residentes de la UE. El incumplimiento de las normas contenidas en este nuevo marco legal puede derivar en multas que alcancen hasta el cuatro por ciento de la facturación mundial de la empresa responsable.

Lo anterior representa, sin duda, un caso de extraterritorialidad en el alcance de esta norma jurídica. Por ello, es importante resaltar las principales aportaciones del nuevo Reglamento.

En primer lugar, se persigue que la nueva regulación constituya un marco jurídico armonizado que procure una aplicación uniforme de la ley en beneficio de un mercado único digital en la Unión Europea.

Como consecuencia de lo anterior, se establece igualdad de condiciones para todas las empresas que operan dentro del mercado de la Unión Europea. Las empresas que realicen estas operaciones desde el exterior de la UE y que reporten actividades dentro de este mercado único deben, en determinadas circunstancias, nombrar un representante en la Unión Europea al que los ciudadanos y las autoridades puedan dirigirse además de a la empresa con sede en el extranjero o a parte de ella.

La reglamentación establece, además, la propuesta de una serie de incentivos para que se adopten las medidas conducentes a encontrar soluciones innovadoras en el tema de protección de datos personales.

Asimismo, se incorporan nuevas garantías para el derecho a la información, acceso y eliminación de datos (derecho al olvido), estableciendo reglas como la que hasta entonces señalaba que la falta de actividad generaba un consentimiento tácito y la protección de los niños en línea.

Una de las novedades que aporta el RGDP es el establecimiento de un derecho de portabilidad de datos que permite a los ciudadanos de la UE solicitar a determinada empresa que le devuelva los datos personales que le concedió por consentimiento o en virtud de un contrato. Asimismo permite que dichos datos personales puedan ser transferidos a otra empresa cuando haya las facilidades tecnológicas para ellos. Lo anterior tiene como finalidad proteger los datos, apoyar la libre circulación de los mismos y evitar las retenciones arbitrarias de los datos personales, además de fortalecer la libre competencia entre empresas al facilitar el cambio de datos personales entre diversos proveedores.

En el RGDP se define claramente lo que se considera jurídicamente una *violación de la seguridad de los datos personales* obligando, en algunos casos, a las empresas a notificar a las personas cuyos datos se ven afectados por la violación.

El Reglamento otorga a todas las autoridades de protección de datos la competencia para establecer multas a los responsables del tratamiento considerando la facultad de imponer multas de hasta veinte millones de euros o, en el caso de una empresa, hasta el cuatro por ciento de su volumen de negocios anual.

El Reglamento transita de un sistema de notificación en caso de violación al derecho de protección de datos personales a un principio de responsabilidad proactiva al crear un sistema de obligaciones graduales en función de los riesgos. Asimismo, se establece un instrumento claro para ayudar a evaluar el riesgo antes de que inicie el tratamiento: la evaluación de impacto relativa a la protección de datos. Dicha evaluación debe realizarse, de

manera obligatoria, cada vez que haya posibilidad de que el tratamiento de los datos represente un riesgo importante para la salvaguarda de los derechos y libertades de las personas.

El RGPD menciona tres situaciones específicas que representan un posible riesgo elevado:

1.Cuando una empresa evalúa de forma sistemática y en profundidad aspectos personales de un individuo,

2.Cuando procesa datos sensibles a gran escala, o;

3.Cuando realiza un control de zonas públicas a gran escala.

Una de las aportaciones que otorga mayor impacto al RGPD es que la protección de los datos personales que se garantiza se desplaza, junto con los datos, al exterior de la Unión Europea, lo que procura un elevado nivel de protección.

Si bien en la Directa de 1995 de la UE sobre Protección de Datos Personales se establecieron principios básicos sobre las transferencias internaciones, el nuevo Reglamento introduce un catálogo muy preciso relativo a los elementos que la Comisión debe tener en cuenta a la hora de evaluar si un sistema extranjero protege adecuadamente los datos de carácter personal.

4.Internet y protección de datos personales, un reto global.

Internet es una herramienta que ha generado progreso social y económico. Tiene como característica su apertura y una tendencia globalizadora en la que la información fluye de manera continua a una velocidad cada vez mayor.

Desde los Estados y los organismos supra e internacionales como la Unión Europea, se ha buscado regular de la mejor manera este desarrollo para garantizar los derechos de las personas físicas y de las personas jurídicas que puedan verse afectadas por este flujo acelerado y sin límites de información.

El tratamiento de prerrogativas iusinformativas tales como la protección a la propia imagen, el derecho al honor y la protección de datos ha sido una preocupación constante en el ámbito nacional e internacional, por ello, y ya que el flujo de datos e información a través de Internet tiene un alcance global, se requiere un enfoque colaborativo entre los Estados y entre organismos internacionales para poder regular actividades que trascienden fronteras físicas y jurídicas estatales.

La protección de los datos personales deriva de que éstos son, además de un objeto inmaterial de propiedad de los individuos, un conjunto de elementos informativos que dan cuenta de características personalísimas de cada individuo que permiten identificarlo; asimismo, representan elementos de gran valor para las instituciones públicas y, especialmente, de gran valor económico para las empresas privadas.

Para las instituciones públicas, los datos personales son insumos básicos para poder desarrollar sus funciones. Recabar datos personales es actividad necesaria para muchas

instituciones de esta naturaleza, por ejemplo, aquéllas que brindan seguridad, las que prestan servicios de salud, las educativas y las recaudatorias.

Por su parte, las empresas privadas utilizan los datos personales, además de para estar en contacto y dar un mejor servicio a su consumidor, para tener un mayor margen de ganancia y para poder competir con otras empresas.

En la sentencia 290/2000[3] el Tribunal Constitucional de España definió el derecho a la protección de datos como un poder para controlar la disposición sobre datos personales que confiere a su titular un conjunto de facultades constitutivos de los elementos de ese derecho fundamental. Esta prerrogativa se integra, también, por los derechos de consentir la obtención y el conocimiento del uso que se dará a los mismos.

El RGPD, en su artículo 3, regula el tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no, así como el tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión.

Para efectos del presente trabajo, la consideración relativa al tratamiento de los datos personales por parte de un responsable que no esté establecido en la Unión es una derivación de gran calado en virtud de que obliga, prácticamente, a todos los Estados, sean o no miembros de la Unión a acatar sus disposiciones cuando se trate del manejo de datos personales de personas físicas residentes en algún Estado miembro de la Unión.

En este contexto, la normativa analizada enriquece el marco jurídico de la protección de datos en América Latina y especialmente en México.

5.México, la protección de datos y la extraterritorialidad del RGDP.

En México, la protección de datos personales se considera un derecho humano reconocido en nuestra Constitución política y reglamentado por dos leyes específicas en la materia.

La Constitución mexicana señala en su artículo 16:

> *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*.[4]

México cuenta con normas que regulan la protección de datos personales que obran tanto en el sector público como en el privado, por lo que ésta forma parte de los países que limitan, por lo menos normativamente, el uso indiscriminado de bases de datos, así como su venta ilícita y carente del consentimiento de los titulares de la información. Así, se han establecido procedimientos para combatir las decisiones que los responsables de bases de datos personales toman sobre las solicitudes de ejercicio de los derechos ARCO.

En México existen 32 órganos locales (uno por cada entidad federativa) y un órgano nacional en materia de protección de datos personales, los cuales encaminan sus esfuerzos al cumplimiento de la legislación correspondiente.

En este país el reconocimiento de la protección de datos personales como un derecho autónomo es bastante reciente. Su primera incorporación en el marco jurídico se dio con la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en el año 2002.

En julio de 2007, se reformó el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos estableciendo que la información que refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Es de señalarse que hasta este momento, la protección de datos personales era una obligación exclusivamente enfocada a los poderes públicos o entes gubernamentales.

El 1º de junio de 2009 se reforma el artículo 16 de la Constitución Política de manera que se reconoce plenamente el derecho de toda persona a la protección de su información.

Así, el artículo 16 señala que

> *Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. 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 que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros*.[5]

La reforma señalada en el párrafo precedente propició que en México se desarrollaran normas especiales en materia de protección de datos personales, así como normas que protegieran de menor manera los derechos de acceso, rectificación, cancelación y oposición de los particulares en el empleo de sus datos (Derechos ARCO).

Por otra parte, se reformó el contenido del artículo 73 de la misma Constitución Federal para otorgar en la fracción XXIX-O al Congreso de la Unión la facultad de legislar en materia de protección de datos personales en posesión de los particulares.

Derivado de todo lo anterior, el 5 de julio de 2010, el Diario Oficial de la Federación[6] publicó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

En 2017 se aprobó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que regula el contenido del artículo 6º base A y 16 de la Constitución mexicana en materia de protección de datos personales.

Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

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 serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares. En todos los demás supuestos diferentes a los mencionados en el párrafo anterior, las personas físicas y morales se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En este país, se cuenta también con regulaciones especiales para cada sector para la protección de datos que se manejan en los mismos. Así se pueden encontrar disposiciones específicas en materia fiscal, financiera y de salud.

México solicitó formalmente, en 2017, a través de su Cancillería la adhesión al Convenio 108 del Consejo de Europa, a efectos de ser considerado como país con niveles óptimos de protección de datos personales, lo cual tiene como objetivo generar un clima de confianza mutua entre la Unión Europea y los sectores comerciales públicos y privados de México y los países miembros de aquella, siempre teniendo en cuenta que el Consejo de Europa y la Unión Europea son dos organizaciones diferentes.

Aunado a lo anterior, se debe destacar que este país integra la Red Iberoamericana de Protección de Datos Personales, en la cual se ha deliberado y se han tomado decisiones importantes en materia de armonización de la protección de datos personales en la comunidad de países iberoamericanos, que han sido tomadas como modelo en México de lo que debe contener la legislación especializada en la materia y del diseño institucional para generar instancias y procedimientos tendientes a proteger los datos personales no solamente de los ciudadanos y residentes mexicanos, sino de aquellas personas físicas y jurídicas colectivas que tengan relaciones comerciales o cualquier otro tipo con empresas públicas y privadas mexicanas que importen la transferencia y manejo de datos de carácter personal. Por ello, se puede afirmar que México no ha sido ajeno al concierto internacional que propugna la armonía y colaboración en materia institucional y legislativa para garantizar de mejor manera la integridad y buen uso de los datos personales.

Si bien, en México, en la última década se ha avanzado con paso firme para fortalecer la protección de datos personales en el sector público, en el sector privado aún existen grandes áreas de oportunidad que es pertinente esbozar de cara a la implementación con plena vigencia del RGPD de la UE para aquellas empresas mexicanas que presten servicios u ofrezcan productos a residentes o ciudadanos de la Unión.

Hay estudios que muestran los desafíos que afronta el sector arriba señalado en materia de protección de datos.[7]

En las siguientes líneas, de manera general, se enuncian los principales desafíos que afrontan las empresas de servicios establecidas en México, en relación con 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.

El Estudio de Protección de Datos Personales entre Usuarios y Empresas de 2012 evaluó tanto a internautas mexicanos como a 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, el 50 % de empresas evaluadas no tiene el conocimiento necesario para su atención y, por lo tanto, podrían ser acreedoras de una sanción por el incumplimiento de las disposiciones de la LFPDPPP.

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

No obstante, el 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, el 50 % de las empresas considera que el cumplimiento de la LFPDPPP genera gastos adicionales.

Señala Mendoza Enríquez que

> *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*.[8]

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, 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.

Aunado a lo anterior, el reto en materia de protección de datos en nuestro país será la implementación efectiva del RGDP.

Para conseguir la plena vigencia de un texto normativo de la naturaleza del RGPD se requiere, además de la voluntad política que ya ha manifestado México, una serie de políticas públicas encaminadas a la difusión del mismo entre los operadores jurídicos encargados de aplicarlo y de observarlo.

Por lo anterior, será fundamental que tanto el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales como sus referentes locales hagan campañas y estructuren capacitaciones para las empresas mexicanas que prestan servicios u ofrecen productos a los residentes en la UE.

Asimismo, es importante destacar que desde el poder legislativo se hacen ya esfuerzos para armonizar la legislación nacional con el contenido del RGPD.

México, desde 2010, ha dado pasos comprometidos con la internacionalización de la protección de los derechos fundamentales. Baste recordar la gran reforma en materia de derechos humanos que llevó a establecer en el artículo 1º de su Carta Fundamental que, en México, se reconocen los derechos humanos contenidos en la misma y con el mismo carácter los contenidos en los tratados internacionales de los que este país será parte. Esta apertura se ha traducido en una mayor flexibilidad del sistema jurídico secundario para armonizar sus contenidos con las directivas y principios emanados del Derecho internacional.

En este contexto positivo, si bien la aplicación del RGPD puede ser un reto, no es un objetivo inalcanzable. Hay muestra de pasos firmes hacia el camino de la mejor garantía de la protección de los datos personales: la cooperación entre países.

En un contexto donde las fronteras jurídicas se difuminan en materia de derechos fundamentales y se fortalece la voluntad internacional de colaborar para protegerlos, México se integra y adopta la plena vigencia del nuevo RGPD de la UE.

Por todo lo anterior, la extraterritorialidad del RGPD de la UE deviene, en primera instancia, una mayor garantía para los usuarios y consumidores de bienes y servicios, tanto para aquellos que residiendo en México opten por el consumo o prestación de servicios de empresas radicadas en la UE como de aquellos europeos que reciban bienes o servicios de empresas mexicanas que teniendo su sede en México tengan actividades comerciales transfronterizas.

Así, podemos detallar, algunos de los efectos que tendrá la aplicación del RGPD en las empresas mexicanas. En primer lugar, encontraremos un impacto comercial porque todas las empresas en México deberán garantizar el cumplimento de las políticas de protección de

datos personales acordes con la nueva regulación europea, sin menoscabo del cumplimiento de la normativa nacional; el incumplimiento de dicha normativa pondría en riesgo las relaciones comerciales, no solamente futuras, sino las ya existentes.

La aplicación del RGPD de la UE tiene un evidente impacto jurídico en México. Esto es así porque se complementa el marco normativo nacional con el internacional. De esta suerte, las empresas mexicanas están obligadas a, en primer lugar, hacer un estudio detallado del nuevo reglamento y, en segundo lugar, a modificar sus políticas internas de protección de datos para ajustarse a esta norma extraterritorial, sin dejar de observar, por supuesto, el marco normativo nacional. Asimismo, las empresas que incumplan con las disposiciones aplicables del RGPD podrán ser sujetas a sanciones por parte de los órganos reguladores del mismo.

Por lo que se refiere a la cultura organizacional de las empresas mexicanas, la implementación del RGPD de la UE implica que cada empresa mexicana que encuadre en el supuesto de aplicabilidad de la citada norma deberá reestructurar su organización interna para fortalecer los espacios que gestionan los datos personales, dotándolos de una estructura y representatividad sólidas en el interior de la propia empresa y de políticas empresariales y procesos internos para garantizar el cumplimento de las disposiciones europeas.

Por todo lo anterior, la aplicación extraterritorial del RGPD de la UE es un ejercicio jurídico que amplía la protección de los datos personales en nuestro país, obligando a las empresas mexicanas que prestan bienes o servicios en la UE o a las empresas europeas que prestan bienes o servicios en nuestro país, a tutelar más eficientemente este derecho, estableciendo la obligación de contar con estructuras sólidas en el interior de cada empresa y con procesos eficientes para el reclamo por eventuales violaciones de los datos personales.

Conclusiones.

1.La protección de datos personales, independientemente de las fronteras geográficas, requiere de la adopción de normas, estándares, procesos y mecanismos uniformes que permitan garantizar el derecho a la protección de datos.

2.La protección de datos debe, tanto a los interesados, como a los responsables del tratamiento de datos, integridad, garantizar la confidencialidad y seguridad, durante y después del término de autorización del manejo de datos.

3.La cooperación internacional es fundamental para el desarrollo de la protección del tratamiento de datos con la finalidad de fortalecer la seguridad y protección uniforme de este derecho.

4.El Reglamento de Protección de Datos de la Unión Europea permite hablar de la urgencia de establecer mecanismos homogéneos de protección de datos, no sólo para Latinoamérica, sino instrumentos de carácter global que aseguren la protección de datos con el fIn de continuar con los retos que implica la evolución tecnológica y económica.

5.El RGPD constituye un verdadero ejercicio de ampliación de garantías al establecer, más allá de los tradicionales derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), nuevos derechos como el derecho al olvido, el derecho a la portabilidad de los datos o el derecho de oponerse al tratamiento de los datos personales con fines específicos.

6.Otra importante innovación es el establecimiento de nuevas obligaciones para los responsables de los datos, tales como denunciar en un plazo no mayor de 72 horas cualquier incidente de seguridad de datos personales, la obligación de designar a un representante a los fines del RGPD con sede en la Unión Europea; designar, en ciertos casos, un agente de protección de datos personales y cláusulas que deben incluirse de manera obligatoria en los contratos con proveedores.

7.México es un país con vocación de cooperación internacional. Muestra de ello es el viraje constitucional y jurisprudencial que se vive desde 2010 en materia de aplicación directa de los tratados internaciones en materia de derechos humanos.

8.Derivado de lo anterior, el RGPD tiene una recepción adecuada en México, si bien su implementación representa retos importantes para las empresas y los agentes jurídicos encargados de observarlo. La autoridad en materia de protección de datos personales ha dado pasos firmes para su armonización con el marco jurídico mexicano.

9.Cada vez hay mayor apertura y flexibilidad del sistema mexicano para recibir y observar normativas internacionales, especialmente aquellas encaminadas a fortalecer los contenidos internos en materia de garantía de los derechos.

10.Finalmente, la aplicación extraterritorial de este Reglamento en México genera una serie de obligaciones jurídicas y organizacionales para la empresa mexicana que oferte bienes o servicios a residentes en la UE o para aquella empresa europea que oferte bienes o servicios en México. Estas obligaciones representan la urgencia de mejorar las estructuras empresariales para dotar a las áreas que manejan datos personales de una mayor capacitación en cuanto a conocimiento y comprensión del Reglamento, de procedimientos más eficientes para el manejo adecuado de los datos y para desahogar las eventuales reclamaciones por la violación de los datos personales.

[1] 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/TXT/?uri=celex:32016R0679 (consultado el 12 de marzo de 2019).

[2] 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. http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf (consultado el 12 de marzo de 2019).

[3] Sentencia 290/2000, Tribunal Constitucional, Pleno, Ponente Magistrado Don Julio Diego González Campos, Boletín Oficial del Estado (BOE), 30 de noviembre de 2000, núm. de recurso 201/1993.
http://hj.tribunalconstitucional.es/es/Resolucion/Show/4274 (consultado el 12 de marzo de 2019).

[4] http://www.ordenjuridico.gob.mx/Constitucion/articulos/16.pdf (consultado el 12 de marzo de 2019).

[5] http://www.ordenjuridico.gob.mx/Constitucion/articulos/16.pdf (consultado el 12 de marzo de 2019).

[6] Órgano oficial para la comunicación institucional y la publicación de contenidos legislativos por parte del Estado mexicano.

[7] Véase el importante estudio de Olivia Andrea Mendoza Enríquez, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", *Revista Ius*, Vol. 12, Núm. 41, Puebla, Ene-Jun 2018.
http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267

[8] Olivia Andrea Mendoza Enríquez, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", Revista Ius, Vol. 12, Núm. 41, Puebla, Ene-Jun 2018 (consultado el 12 de marzo de 2019).

Legislación

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (2016).
Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679 (consultado el 31 de enero de 2019).

Bibliografía y documentación

ACUÑA LLAMAS, F. J. *La protección de los datos personales y notas sobre los desafíos de Internet.*
https://www.sitios.scjn.gob.mx/cec/sites/default/files/archivos/calendario_actividades/06_ACU%C3%91A_La%20constitucion%20en%20la%20sociedad%20y%20economia%20digitales.pdf (consultado el 12 de marzo de 2019).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *El impacto del Reglamento General de Protección de Datos sobre la actividad de las administraciones públicas*. Recuperado de https://www.aepd.es/media/docs/impacto-rgpd-en-aapp.pdf (consultado el 31 de enero de 2019.

ASOCIACIÓN MEXICANA DE INTERNET. *Estudio de protección de datos personales entre usuarios y empresas.*
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= (Consultado: 31 de enero de 2019).

ASOCIACIÓN MEXICANA DE INTERNET. *Estudio sobre el valor económico de los datos personales.*
Disponible en: https://amipci.org.mx/images/valor_eco_Datospersonales_FINAL.pdf
(consultado el 13 de mayo de 2017).

EL ECONOMISTA. *Reglas europeas de protección de datos*. Recuperado de https://www.eleconomista.com.mx/internacionales/Reglas-europeas-de-proteccion-de-datos-con-efecto-en-todo-el-mundo-20180515-0038.html (consultado el 31 de enero de 2019).

EUROPEAN UNION. Your Europe; Protección de datos.
Recuperado de https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_es.htm (consultado el 31 de enero de 2019).

MENDOZA ENRÍQUEZ, O. (2013). *Implicaciones jurídicas de la protección de datos personales en medios electrónicos de la empresa en México. Derecho del Teletrabajo.* México/ Popocatépetl.

MENDOZA ENRÍQUEZ, O. (2018). "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento". *Revista Ius,* vol. 12, Núm. 41, Puebla, Ene-Jun.

SECRETARÍA DE ECONOMÍA. *Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI.*
Disponible en:https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_04.pdf (consultado el 30 de abril de 2017).