Instituto IDEAS

INSTITUTO DE ECONOMÍA APLICADA Y SOCIEDAD

innovación y tecnología

Protección de datos personales

JULIO 2020

Sofía Quesada

Gretel Zeniquel

@Institutoldeas_ Insituto IDEAS @Institutoldeas_

RESUMEN

Hoy en día los datos constituyen un activo más con el que cuentan las empresas y plataformas digitales. La recopilación de vastas cantidades de información de los usuarios digitales se ha convertido en una práctica habitual, y con ella surgieron problemas respecto de su regulación legal. A lo largo de los últimos años, se ha comprobado que entidades de los sectores público y privado han usado la información con propósitos distintos a aquellos por los que les fue confiada originalmente. Por esta razón, distintos Estados están realizando esfuerzos para reducir el impacto de esas prácticas.

Tema

En el mundo existen diferentes declaraciones, tratados y leyes que protegen a los ciudadanos en cuanto al uso que le dan las empresas y plataformas digitales a su información personal. Estas disposiciones incluyen sanciones económicas a aquellas entidades que filtren o vendan datos personales de terceros; establecen la formación de organismos que asesoren a ciudadanos que se vieron perjudicados por el mal uso de su información privada e incluso promueven la educación sobre el uso de datos dirigida a ciudadanos, para conocimiento de las leyes y de sus propios derechos.

Subtema

Este artículo se propone analizar las diferentes disposiciones legales promulgadas para regular a las empresas y/o plataformas digitales con respecto al uso que le dan a la información privada de los ciudadanos. Se dispone a examinar las reglamentaciones y leyes sancionadas dentro de la Unión Europea; Estados Unidos y Argentina.

Unión Europea

Con respecto a la Unión Europea cabe destacar el Reglamento General de Protección de Datos (GDPR), el cual se promulgó en abril de 2016 y entró en vigencia

el 25 de mayo del 2018.[1] "Se trata de un riguroso marco legal que establece lineamientos en términos de protección de datos para empresas y gobiernos, así como elevadas multas para quienes no cumplan con ellos. Estas pueden llegar hasta los 20 millones de euros o el 4% de las ganancias anuales de la compañía a nivel global, y han alcanzado a gigantes como Google, Facebook o British Airways".[2] "El GDPR se aplica a cualquier forma de datos personales, definida como cualquier dato que por sí mismo, o cuando se combina con otros datos a los que el poseedor pueda acceder, puede usarse para identificar a un individuo".[3] "La ley europea también incluye regulaciones que protegen datos sensibles -bajo protección constitucional a nivel europeo- y prohíben su entrega, aún en los casos donde los usuarios dieran su consentimiento. En otras palabras, los protege de sí mismos".[4]

"El GDPR está destinado a ser una ley integral de privacidad de datos para los países miembros de la UE, pero cada país debe aprobar sus propias regulaciones para monitorear y hacerla cumplir dentro de sus fronteras".[5] El organismo europeo encargado de monitorear el debido cumplimiento de la legislación sobre protección de datos es el Supervisor Europeo de Protección de Datos (SEPD), el cual supervisa el cumplimiento de las normas de esta índole en las instituciones europeas además de investigar las denuncias. Por otro lado, la UE cuenta con el Consejo Europeo de Protección de Datos (CEPD), el cual tiene personalidad jurídica y secretaría propia, además de tener rango de organismo de la UE. El CEPD tiene competencia en litigios entre las autoridades nacionales de supervisión, además de tener competencias para asesorar y orientar sobre las normativas de protección de datos vigentes. A nivel nacional existen las Autoridades de Protección de Datos (APD), las cuales funcionan de manera independiente y son de carácter público. Cada país miembro designa a su representante.[6]

El GDPR no sólo favorece a los ciudadanos al fortalecer sus derechos fundamentales, sino que también beneficia a las empresas al simplificar las normas que se les aplican

[1] Bio, Damian. (2019). Expertos en protección de datos piden modificar la ley: "Corremos el riesgo de ser manipulados por empresas o gobiernos". Buenos Aires, Argentina.: Infobae. Recuperado de: https://www.infobae.com/politica/2019/09/21/expertos-en-proteccion-de-datos-piden-modificar-la-ley-corremos-el-riesgo-de-ser-manipulados-por-empresas-o-gobiernos/

[2] Ídem.

[3] Stranier, Sherwood. (2019). Leyes Globales De Privacidad De Datos: USA, UE, China Y Más. Drfrag This. Recuperado de: https://blog.ipswitch.com/es/leyes-globales-de-privacidad-de-datos-usa-ue-china-y-m%C3%A1s

[4] Bio, Damian. (2019).

[5] Stranier, Sherwood. (2019).

[6] La protección de datos en la UE. Recuperado de: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es

en el mercado único digital, introduciendo una norma única para todo el continente europeo.[7]

Según Estelle Massé, analista de políticas globales de Access Now, una ONG dedicada a defender la protección de los derechos digitales de los usuarios alrededor del mundo, se observan efectos positivos en la práctica: "en el último año hubo un aumento del 60% al 70% en el número de quejas efectuadas por ciudadanos. Esto demuestra que la ciudadanía comprendió sus derechos y están haciendo un mejor uso de ellos, lo que llevará a cambios en las prácticas, dado que la ley está haciendo efecto".[8]

Estados Unidos

Este país constituye un caso particular ya que es la única potencia en carecer de un conjunto unificado de leyes nacionales de privacidad de datos. Estados Unidos posee una disposición legal en esta temática: la Ley de Privacidad del Consumidor de California (CPA), la cual sólo tiene injerencia en el estado de California y está inspirada en el GDPR de la Unión Europea.[9] Esta normativa entró en vigencia en enero de 2020 y estipula que si una empresa vende o compra datos de al menos 50.000 residentes de California en un año; o si sus ingresos superan los 25 millones de dólares o si la mitad de sus ingresos provienen de la venta de datos personales de sus clientes, la empresa deberá manifestar qué categorías de datos está recopilando y qué está haciendo con los datos de sus clientes.[10]

"El CPA de California responsabiliza a todas las empresas del manejo seguro de los datos personales. También exige que los usuarios estén informados sobre cómo se usan esos datos y si éstos se ven comprometidos de alguna manera".[11] "Esta ley es la primera de Estados Unidos que otorga a los consumidores control sobre el uso que las empresas privadas hacen de sus datos personales, otorgándoles a los clientes la posibilidad de solicitar a la empresa que prohíba el envío de sus datos personales a terceros, o que eliminen dichos datos del sitio. Esta reglamentación establece multas de hasta u$s7.500 a aquellos que no la cumplan, y corresponde al Fiscal General la facultad de establecer reglas y procedimientos sobre cómo procesar y cumplir con las solicitudes verificables de los consumidores de información personal específica, con el

[7] La protección de datos en la UE. Recuperado de: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es

[8] Bio, Damian. (2019).

[9] Stranier, Sherwood. (2019).

[10] Renter Molins, Albert. (2020). La primera ley de privacidad en línea de EE.UU. entra en vigor en California. Barcelona, España.: La Vanguardia. Recuperado de: https://www.lavanguardia.com/vida/20200105/472713380363/california-estados-unidos-privacidad-consumidor-e-commerce-comercio-electronico.html

[11] Stranier, Sherwood. (2019).

objetivo de abordar los obstáculos a la implementación y las preocupaciones de privacidad".[12]

"Estados Unidos también acordó un conjunto mínimo de estándares de privacidad, según lo definido por el Foro de Cooperación Económica Asia-Pacífico (APEC), el cual está integrado 21 países, incluidos Japón; Canadá y México. Este conjunto de estándares dio lugar a la formulación de Las Reglas de Privacidad Transfronterizas (CBPR), las cuales se establecieron para proporcionar una base para las leyes de privacidad dentro de cada uno de los países miembros de APEC. Las pautas de privacidad de datos de CBPR se aplican a cualquier organización pública o privada que maneje datos personales y está destinado a proporcionar un nivel mínimo de protección, útil para los países miembros que comercian dentro del grupo. Depende de los Estados miembros para construir sobre ese marco con reglas para sus mercados específicos".[13]

Argentina

Este país dispone de un marco normativo referido a la protección de datos personales formado por el artículo 43 de la Constitución Nacional, el cual dispone: "Toda persona podrá interponer acción expedita y rápida de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística." Por otro lado, Argentina posee también la Ley de Protección de los Datos Personales (Ley N° 25.326), sancionada el 4 de octubre del 2000. Existe a su vez el Decreto 1558/2001 de reglamentación de la ley de protección de datos personales y la Resolución 47/2018 de la Agencia de Acceso a la Información Pública (AAIP), sobre medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados y no informatizados.

"El 19 de septiembre de 2018, el Poder Ejecutivo Nacional presentó el Proyecto MEN-2018-147-APN-PTE con la intención de sustituir la Ley de Protección de Datos Personales N° 25.326 promulgada en el año 2000".[14] "La iniciativa sigue la mayoría de los lineamientos del GDPR y, de hecho, uno de sus objetivos centrales es implementar una cantidad suficiente de regulaciones para ser considerado "país adecuado" por la UE.

[12] Renter Molins, Albert. (2020).

[13] Stranier, Sherwood. (2019).

[14] Giay P, Fernández y Peruzzotti. (2018) Proyecto de Ley de Protección de Datos Personales. Buenos Aires, Argentina.: Marval, O'Farrell y Mairal. Recuperado de: https://www.marval.com/publicacion/proyecto-de-ley-de-proteccion-de-datos-%20%20%20%20%20%20personales-13237

El proyecto aún no se aprobó. En Argentina el control de los datos personales por parte del Estado es ejercido por un funcionario que depende del Poder Ejecutivo y tiene un limitado margen de autonomía".[15]

"Durante 2016, la Agencia de Acceso a la Información Pública (AAIP), en ese entonces denominada Dirección Nacional de Protección de Datos Personales (DNPDP), impulsó un proceso de reflexión respecto de la necesidad de reformar la Ley 25.326 de Protección de Datos Personales".[16] "Posteriormente se llevó a cabo la redacción de un anteproyecto de reforma de ley que tiene dos versiones, siendo la última de éstas de febrero de año 2017 ya que existen riesgos de continuar con la ley vigente, debido a que ésta implica un peligro muy grande para el proceso electoral y los gobiernos podrían acceder a información y bases de datos usadas con propósitos de gestión".[17]

Los principales cambios que plantea el anteproyecto de reforma de Ley de Datos Personales es:

- "La incorporación de delegados, los cuales deben notificar incidentes en materia de seguridad y comunicación de los datos. La figura del delegado será obligatoria para algunas empresas, sin especificar aún cuáles."[18]
- "El anteproyecto también plantea un consentimiento "mixto", expreso e informado por parte del titular de los datos. Éste debe saber qué se hace con su información privada. Según Johanna Faliero, abogada en Derecho Empresarial y Privado, especialista en Derecho Informático, "nuestra redacción del anteproyecto recepta un sistema de consentimiento; porque admite tanto el consentimiento expreso como tácito". El consentimiento tácito es "blanquear" o dar por entendido que cuando un usuario navega en internet, acepta muchas de estas condiciones".[19]
- "No hay Derecho al Olvido. La redacción del anteproyecto de reforma de la ley de Datos Personales no incorpora el Derecho al Olvido, contemplado en el GDPR. Éste permite que un usuario solicite la eliminación (desindexación) de sus datos personales por diferentes motivos. A pesar de no contemplar el derecho al olvido, la Ley vigente considera excepciones en donde el usuario puede solicitar que se borren contenidos falsos o inexactos, por ejemplo, a través del Artículo 16 (Derecho de rectificación, actualización y supresión). Mientras que el Artículo 17 plantea excepciones, en donde los responsables o usuarios de bancos de datos pueden denegar el acceso, rectificación o la supresión del contenido, "en función de la protección de la defensa de la Nación, del orden

[15] Bio, Damian. (2019).
[16] Schulkin, Julieta. (2018).
[17] Bio, Damian. (2019).
[18] Schulkin, Julieta. (2018).
[19] Ídem.

y la seguridad públicos, o de la protección de los derechos e intereses de terceros"".[20]

- También se establecen modificaciones en lo que respecta a la transferencia internacional de datos. "Hoy, a través de la ley vigente, si el titular de los datos da su consentimiento, podría realizarse la transferencia internacional de sus datos, aun si fueran destinados a un país con niveles no adecuados (no seguros) de protección de datos. - El anteproyecto suma alternativas. La transferencia internacional de datos planteada, apunta a no enviar los datos personales a un país que no tenga la protección adecuada como la Argentina. ¿Qué sucede con los datos alojados en servidores extranjeros? Alejandro Anderlic, Director de Legales y Asuntos Corporativos de Microsoft explica que "Si los datos se transfieren a una jurisdicción que la ley argentina hoy considera que no brinda adecuada protección -como es el caso de Estados Unidos-, quien transfiere los datos debe firmar con el proveedor extranjero un acuerdo de transferencia internacional de datos (Data Transfer Agreement o DTA por sus siglas en inglés)"".[21]
- Se incorporan, además, una serie de definiciones nuevas como, por ejemplo, datos biométricos y genéticos.[22]
- También se tiene en cuenta el organismo estatal que se encargaría de monitorear su cumplimiento, el cual sería la Agencia de Acceso a la Información Pública ya que "ésta garantiza el derecho de acceso a la información pública, promueve medidas de transparencia activa y la protección de los datos personales. Por lo tanto, sería responsable de gestionar los reclamos y de guiar a los ciudadanos ante cualquier eventualidad que involucre la vulneración de sus datos".[23]

Sin embargo, a pesar de los cambios que se describieron anteriormente, el proyecto presenta una serie de falencias:

- "Permite el tratamiento de datos para el cumplimiento de funciones y competencias del Estado o para los casos de "protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros". Esto implica que sería el propio Estado quien determinaría cuándo se cumplen los requisitos para usar los datos con un propósito distinto al original".[24]

[20] Schulkin, Julieta. (2018).
[21] Ídem.
[22] Ídem.
[23] Ídem.
[24] Bio, Damian. (2019).

- Además, está la "necesidad de endurecer las sanciones previstas en el proyecto. En contraste con la ley europea, el proyecto establece multas bajas sin carácter disuasorio, lo que puede implicar la falta de cumplimiento de la ley por parte de grandes empresas".[25]
- También es "necesario contar con autoridades de control verdaderamente independientes. A lo largo de los años se sucedieron distintas figuras que funcionaron como organismo de control -desde 2016 es la Agencia de Acceso a la Información Pública- pero todas continuaron bajo la esfera del Ejecutivo. Y el proyecto tampoco prevé cambiarlo".[26]
- Otra de las falencias del proyecto es que "sólo sea necesario comunicar a los usuarios las filtraciones de datos o incidentes de seguridad cuando sea probable que entrañe altos riesgos a sus derechos', lo que implica excesivo margen de actuación a las empresas ya que son estas mismas las que evaluarán ese riesgo".[27]
- Otra de las cláusulas problemáticas, "es el consentimiento informado de los titulares de los datos. El consentimiento tácito es un peligro, una trampa. Puede darse mediante la simple aceptación de términos de uso".[28]
- Por último, "el proyecto habilita el tráfico de datos de subsidiarias, de empresas que toman datos aquí y tienen sus casas matrices en otros países. Esto es una cláusula muy apropiada para los negocios de las grandes empresas transnacionales que tienen en los datos personales y su cruce, el insumo principal de su negocio, los Facebook, Instagram, Google. Esta cláusula tira abajo, de algún modo, las protecciones nacionales que podemos tener de los datos personales".[29]

Conclusión.

En los tiempos digitales que corren hoy en día, la información es el commodity más importante. La mayor parte de los países del mundo carece de legislaciones que regulen el manejo de datos personales, por lo tanto existe un campo abierto a la hora de abordar esta temática. No obstante, el Reglamento General de Protección de Datos (GDPR), impulsado por la Unión Europea funciona como sustento legal y los países lo utilizan como base de su marco normativo con respecto a la protección de datos personales. Como se desarrolló en el presente trabajo, las diferentes

[25] Bio, Damian. (2019).
[26] Ídem.
[27] Ídem.
[28] Schulkin, Julieta. (2018).
[29] Ídem.

disposiciones legales promulgadas para regular a las empresas y/o plataformas digitales con respecto al uso que le dan a la información privada de los ciudadanos, especialmente en Argentina, han quedado desactualizadas. Por lo que es sustancial, volver a poner en marcha el proyecto de ley que modifica la legislación vigente y que perdió estado legislativo en febrero del corriente año, haciendo hincapié en las falencias que se han mencionado anteriormente. Es, a su vez, fundamental que los marcos normativos que surjan estén acompañados por políticas públicas, las cuales van a ser imprescindibles para la debida aplicación de una ley de estas características.

Referencias.

- Bio, Damian. (2019). Expertos en protección de datos piden modificar la ley: "Corremos el riesgo de ser manipulados por empresas o gobiernos". Buenos Aires, Argentina.: Infobae. Recuperado de: https://www.infobae.com/politica/2019/09/21/expertos-en-proteccion-de-datos-piden-modificar-la-ley-corremos-el-riesgo-de-ser-manipulados-por-empresas-o-gobiernos/
- Giay P, Fernández y Peruzzotti. (2018) Proyecto de Ley de Protección de Datos Personales. Buenos Aires, Argentina.: Marval, O'Farrell y Mairal. Recuperado de: https://www.marval.com/publicacion/proyecto-de-ley-de-proteccion-de-datos-%20%20%20%20%20%20%20personales-13237
- La protección de datos en la UE. Recuperado de: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es
- Renter Molins, Albert. (2020). La primera ley de privacidad en línea de EE.UU. entra en vigor en California. Barcelona, España.: La Vanguardia. Recuperado de: https://www.lavanguardia.com/vida/20200105/472713380363/california-estados-unidos-privacidad-consumidor-e-commerce-comercio-electronico.html
- Schulkin, Julieta. (2018). En la era de la big data, cuáles son los 5 cambios que buscan modernizar la Ley de Protección de Datos Personales. Buenos Aires, Argentina.: Infobae. Recuperado de: https://www.infobae.com/tecno/2018/06/23/en-la-era-de-la-big-data-cuales-son-los-5-cambios-que-buscan-modernizar-la-ley-de-proteccion-de-datos-personales/

- Stranier, Sherwood. (2019). Leyes Globales De Privacidad De Datos: USA, UE, China Y Más. Drfrag This. Recuperado de: https://blog.ipswitch.com/es/leyes-globales-de-privacidad-de-datos-usa-ue-china-y-m%C3%A1s