¿QUÉ ES GDPR?

LUIS ARANCIBIA

Abogado. Actualmente se desempeña en la Administración del Dominio .CL (NIC Chile) en el área de gestión de resolución de controversias por nombres de dominio .CL, entre otras materias. Miembro del Directorio de la Asociación de ccTLD´s de América Latina y el Caribe.

lam@nic.cl

INTRODUCCIÓN

El 2018 podrá ser recordado como un año clave en la protección de datos en todo el mundo. A partir de enero de 2018, más de 100 países han promulgado una legislación integral de protección de datos, y alrededor de 40 países están en proceso de establecer dichas leyes[1] y [2].Nuestro país no ha estado ajeno a dicho proceso. El 15 de mayo de 2018 se aprobó una reforma a la Constitución, la cual estableció explícitamente el derecho a la protección de datos personales como un derecho de rango constitucional, al tiempo que se encuentra en actual discusión el proyecto de ley para una nueva ley de datos personales, que pretende sustituir el régimen establecido por la ley 19.628 sobre Protección de Datos de Carácter Personal de agosto de 1999.

En este contexto se despliega -si es que acaso no es el gatillador de dicho proceso- el Reglamento de Protección de Datos de la Unión Europea, también conocido como GDPR, el cual podría ciertamente convertirse en un modelo para el resto del mundo, ya que muchas empresas globales prestan servicio a usuarios en y hacia la Unión Europea. De este modo, dichas empresas y otras organizaciones tendrán que adaptarse a estas reglamentaciones de todos modos, y podría tener sentido adoptar los principios de la norma europea de privacidad digital en todo el mundo[3].

El GDPR es, sin duda, el desarrollo regulatorio más importante en materia de protección de datos personales vigente hasta la fecha. Basado en un mecanismo detallado y protector, está influyendo en el uso de los datos personales y a muchas legislaciones en todo el mundo. Entendido correctamente, el GDPR alentará a las empresas a desarrollar marcos precisos y explícitos de gestión de la información, a utilizar los datos personales en base a una práctica que las obligará a mantener a los titulares de los datos informados sobre la toma de decisiones respecto de ellos. Para alcanzar estos objetivos, el GDPR utiliza criterios y herramientas jurídicas y procedimentales, que serán los factores estructurales que facilitarán la comprobación de violaciones, a la vez que pondrá en tela de juicio a algunos modelos de negocio concebidos en base al uso intensivo de información de personas.

ANTECEDENTES

GDPR es la abreviatura que refiere al General Data Protection Regulation, conocido también como el Reglamento de Protección de Datos de la Unión Europea que entró en vigencia el 25 de mayo de 2018.

El GDPR es la nueva regulación europea para la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos, el cual fue adoptado como Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo de la Unión Europea el 27 de abril de 2016[4] y [5].

El Reglamento es directamente aplicable en todos los estados miembros de la Unión a partir del 25 de mayo de 2018 y está diseñado para reforzar los mecanismos de protección del derecho fundamental de las personas físicas en relación con el tratamiento de sus datos personales[6]. En base a ello, el Reglamento reconoce que los principios y normas relativos a la protección de las personas físicas, en lo que respecta al tratamiento de sus datos

1. Banisar, David. *National Comprehensive Data Protection/Privacy Laws and Bills 2018* (January 25, 2018), disponible en: https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

2. Algunos países tienen leyes de privacidad que se aplican a ciertas áreas, por ejemplo, para niños o registros financieros, pero no tienen una ley integral sobre protección de datos. En los países donde no existe un marco integral de protección de datos, la protección de datos está regulada por leyes sectoriales. Por ejemplo, a pesar de ser un líder temprano en el campo de la protección de datos, la Ley de Privacidad de Estados Unidos de 1974 se aplica únicamente al Gobierno Federal y las leyes posteriores se aplican a sectores o grupos específicos de personas (por ejemplo, la Ley de Protección de la Privacidad en Línea de los Niños). Hasta la fecha no existe una ley integral de protección de datos. Sin embargo, dentro del proceso descrito cabe mencionar la entrada en vigencia de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, del 18 de agosto de 2017. Ver: A Guide for Policy Engagement on Data Protection. PART 1: Data Protection, Explained, disponible en https://www.privacyinternational.org/

3. Una crítica a esta posibilidad, véase Chakravorti, Bashar: *The rest of the world can't free ride on GDPR, disponible en https://www.weforum.org/agenda/2018/05/why-the-rest-of-the-world-can-t-free-ride-on-europe-s-gdpr-rules*

4. El texto oficial puede obtenerse en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

5. Junto al GDPR, la reforma consideró también la aprobación de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

6. De acuerdo al sistema de fuentes del Derecho de la Unión Europea, un Reglamento tiene alcance general, es obligatorio en todas sus partes y directamente aplicable en cada estado miembro. Los destinatarios, esto es, personas, estados miembros e instituciones de la Unión, deberán acatar los Reglamentos en su totalidad como "ley de la Comunidad". Un Reglamento es directamente aplicable en todos los estados miembros, sin necesidad de un acto nacional de adopción. Desde su entrada en vigor, se impone en todos los ordenamientos jurídicos nacionales. Una Directiva, en cambio, obliga al estado miembro destinatario en cuanto al resultado que debe conseguirse y son ellos los que eligen la forma y los medios para la adopción de sus términos. Para que los objetivos contemplados en la Directiva tengan efecto para los ciudadanos es preciso que el legislador nacional proceda a un acto de transposición o "medida ejecutiva nacional", mediante el cual el Derecho nacional se adapta a los objetivos determinados en la misma. Borchardt, Klaus-Dieter. *El ABC del Derecho de la Unión Europea*. Oficina de Publicaciones de la Unión Europea. 2011, p. 93.

de carácter personal deben respetar sus libertades y derechos fundamentales, cualquiera que sea su nacionalidad o residencia.

El GDPR deroga la Directiva 95/46/CE del Parlamento Europeo y del Consejo, en función de armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de dichos datos entre los estados miembros. Tal como sostiene uno de los considerandos del Reglamento[7], aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada ni ha evitado la inseguridad jurídica o una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular en relación a sus actividades en línea. Las diferencias en el nivel de protección en los estados miembros respecto del derecho a la protección de los datos de carácter personal, pueden impedir la libre circulación de éstos en la Unión. Estas diferencias pueden convertirse, por lo tanto, en un obstáculo al ejercicio de las actividades económicas, deteriorar la competitividad e impedir que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión. Esta diferencia en los niveles de protección se debió a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE[8].

El nuevo estatuto se establece para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, en consideración a la determinación de un nivel de protección equivalente, coherente y homogéneo en todos los estados miembros, sin perjuicio de que, en lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los estados deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del Reglamento. Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los estados miembros cuentan con distintas normas sectoriales en ámbitos que precisan disposiciones más particulares. El Reglamento reconoce también un margen de maniobra para que los estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el Reglamento no excluye el Derecho de los estados miembros que determina las circunstancias relativas a situaciones especiales de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito.

Al tener un impacto directo en todos los estados miembros, el GDPR hará que muchos de ellos deban modificar sus leyes nacionales para regular aspectos tales como la posición de la Autoridad de Protección de Datos, las reglamentaciones sectoriales, las normas de transición o las implementaciones de requisitos adicionales en los casos en que el GDPR otorga discreción. Ya se han publicado los primeros proyectos de leyes nacionales con los cambios legislativos necesarios, por ejemplo, en Alemania, los Países Bajos y Polonia.

PRINCIPALES CONTENIDOS DEL GDPR

El Reglamento diseña un modelo de políticas de la Unión Europea en materia de protección de datos personales. Aunque se mantienen los principios de la Directiva 95/46/CE, se han propuesto cambios importantes a las políticas imperantes, que crean un estado de cosas nuevo en el estatuto del tratamiento de los datos personales, con un alto impacto en muchas industrias europeas y globales.

A continuación se expone un resumen de los principales aspectos del GDPR.

(A) MAYOR ALCANCE TERRITORIAL (APLICABILIDAD EXTRATERRITORIAL)

El Reglamento aplica a todo el procesamiento de datos personales de personas físicas que permanezcan en la Unión, independientemente de la ubicación de la empresa. En este aspecto el propósito de la regulación es clara: el GDPR se aplicará al procesamiento de datos personales que realicen controladores y procesadores en la Unión Europea, sin importar si el proceso de tratamiento de los datos tiene lugar o no en este espacio. Asimismo, también se aplicará al procesamiento de datos personales de personas en la UE por un controlador o procesador no establecido en la Unión, donde las actividades de cualquiera de aquellos se relacionan con la oferta de bienes o servicios a interesados de la UE (independientemente de si se requiere o no pago) o el control de su comportamiento en la medida que tenga lugar dentro de la UE[9].

7. Véase considerando 1º a 12º del texto del Reglamento.

8. La versión de la Directiva es accesible en: http://www.wipo.int/wipolex/es/details.jsp?id=13580. Una explicación de sus principales aspectos puede consultarse en Cerda, Alberto. Determinación informativa y leyes de protección de datos. Revista Chilena de Derecho Informático. Nº3, Diciembre, 2003. Disponible en http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492,SCID%253D14331%2526ISID%253D507,00.html

9. El Reglamento distingue entre ámbito de aplicación material y territorial. Sobre el Ámbito de Aplicación Material del Reglamento, véase nuestro artículo http://www.laleyaldia.cl/?p=5308

(B) RÉGIMEN DE SANCIONES

Las organizaciones que infrinjan el GDPR, podrán ser multadas con hasta el 4% de la facturación global anual o €20 millones (lo que sea mayor), de acuerdo a lo señalado en el artículo 83, número 5. Ésta es la multa máxima que se puede imponer por las infracciones más graves, como por ejemplo, el no haber obtenido el suficiente consentimiento del interesado para procesar sus datos. Existe un esquema escalonado de multas. A su vez, es importante tener en cuenta que estas reglas se aplican tanto a los controladores como a los procesadores, lo que significa que las "nubes" no estarán exentas de la aplicación de GDPR.

(C) EL CONSENTIMIENTO

El GDPR fortalece las condiciones del consentimiento, el cual se somete un régimen de mayor rigor. Con los nuevos criterios, se terminará con el consentimiento tácito. En este sentido, se deberá entender por consentimiento del interesado a toda manifestación de voluntad libre, específica, informada e inequívoca por la cual el sujeto acepta, ya sea por una declaración o una clara acción afirmativa, el tratamiento de los datos que le conciernen. El consentimiento debe ser claro y distinguible de otros asuntos y proporcionado en una forma inteligible y de fácil acceso, usando un lenguaje claro y sencillo. El interesado tendrá derecho a retirar el consentimiento en cualquier momento. En términos del GDPR, deberá ser tan fácil retirar el consentimiento como darlo.

(D) DERECHOS DE LOS INTERESADOS

d.1. Notificación de filtración de datos. Bajo el GDPR, la notificación por filtración de datos será obligatoria en todos los estados miembros cuando sea probable que esta violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas. En estos casos, el responsable del tratamiento comunicará la probable violación dentro de las 72 horas de

haberla constatado por primera vez. Los procesadores de datos también deberán notificar a sus clientes, los controladores, "sin demora indebida" después de tomar conocimiento por primera vez de una violación de datos[10].

d.2. Derecho de acceso. Consiste en el derecho de cualquier interesado para obtener la confirmación del controlador de los datos si los datos personales que los conciernen se están procesando, dónde y con qué propósito. Además, el controlador deberá proporcionar una copia de los datos personales, sin cargo, en un formato electrónico.

d.3. Derecho de supresión o el derecho al olvido. Conocido como borrado de datos, el derecho a ser olvidado da la posibilidad al interesado a solicitar que el responsable del tratamiento elimine sus datos personales, cese la diseminación de ellos y, potencialmente, haga que terceros detengan el procesamiento de los mismos. Incluso, en determinados casos, el destinatario de la petición deberá proceder sin dilación indebida, por ejemplo cuando los datos personales ya no sean necesarios para los fines para los que fueron recogidos o tratados, o cuando ellos fueron tratados ilícitamente. Sin embargo, este derecho está limitado y no aplica cuando sea necesario conservar los datos por razones de interés público para fines de investigación científica, histórica o estadísticos, entre otros.

d.4. Derecho a la portabilidad de datos. Entendida como la facultad del interesado de recibir los datos personales que le conciernen, que previamente ha proporcionado, en un formato estructurado, de uso común y lectura mecánica, así como el derecho a transmitir esos datos a otro controlador, sin posibilidad de que el anterior detentador de los mismos pueda impedirlo.

(E) PRIVACIDAD POR DISEÑO

La privacidad por diseño implica la exigencia de la inclusión de la protección de datos desde el inicio del diseño de los sistemas, en lugar de ser una adición. Más concretamente, el responsable del tratamiento deberá aplicar las medidas técnicas y organizativas adecuadas de manera efectiva para cumplir los requisitos del Reglamento y proteger los derechos de los interesados. El artículo 25 exige que los controladores retengan y procesen solo los datos absolutamente necesarios para el cumplimiento de sus funciones (minimización de datos), y que limiten el acceso a los datos personales a quienes necesitan representar el procesamiento.

(F) DELEGADOS DE PROTECCIÓN DE DATOS

Bajo las reglas de la Directiva, los controladores están obligados a notificar sus actividades de procesamiento de datos a las Autoridades de Protección de Datos locales, lo que, por ejemplo, para las multinacionales, puede ser una pesada carga burocrática, ya que la mayoría de los estados miembros tienen requisitos de notificación diferentes. Bajo el GDPR no será necesario enviar notificaciones de actividades de procesamiento de datos a cada Autoridad local, ni será un requisito notificar u obtener aprobación para transferencias. En su lugar, habrá requisitos internos de mantenimiento de registros y el nombramiento de un Oficial de Protección de Datos será obligatorio solo para aquellos controladores y procesadores cuyas actividades centrales consisten en operaciones de procesamiento que requieren un monitoreo regular y sistemático de datos a gran escala o de especiales categorías de datos o datos relacionados con condenas y delitos penales. Es importante destacar que el Delegado deberá nombrarse en función de las cualidades profesionales y, en particular, de los conocimientos especializados sobre legislación y prácticas de protección de datos, entre otros requisitos, expresados en el artículo 37 de GDPR. ■

10. Estas reglas han sido puestas en práctica en el reciente incidente sufrido por British Airways, que reveló el jueves 6 de septiembre de 2018 que su sitio web y aplicación fueron víctimas del mayor hackeo que ha sufrido. El ataque es el primero en golpear a una compañía bajo las nuevas regulaciones del GDPR. La compañía, de acuerdo a los reportes de la prensa, habría notificado a la Oficina del Comisionado de Información y a los clientes dentro de las 72 horas obligatorias del Reglamento, sin perjuicio de estar bajo investigación sobre si hubo incumplimiento, lo que en caso de ser efectivo, podría implicar que la empresa sea penalizada si no toma todas las medidas necesarias para proteger los datos de los clientes.
Ver: https://hipertextual.com/2018/09/british-airways-afectados-hackeo