



Protección de datos en Europa

Mariano Corbino¹

Luego de la noticia de que la red social Facebook utilizara de manera indebida los datos de más de 70 millones de usuarios y que los mismos sean utilizados para influir en ciertas decisiones de los mismos, en el Continente europeo a partir del 25 de mayo de 2018 se comenzará a aplicar el nuevo Reglamento General de *Protección de Datos* impuesto por la Unión Europea (GDPR) que mejorará la protección de datos personales.

Debido a la actual legislación y el crecimiento rápido de las nuevas tecnologías existe una inseguridad jurídica en las empresas no solo en cuanto a los límites, procedimientos, transferencias y sobre todo a los métodos de resguardo de los datos personales.

Se espera que el impacto del cambio sea de tal magnitud para las organizaciones si administrasen los datos de manera que puedan poner en riesgo la privacidad de los usuarios, que se habla de sanciones de aproximadamente hasta un 4% de sus ingresos globales.

Ahora bien, el GDPR 2016/679 del Parlamento Europeo y del consejo que fuera aprobado en el año 2016, más precisamente el día 27 de abril, hace referencia a la protección de personas físicas que sustituirá a la Directiva de protección de datos (oficialmente Directiva 95/46 / CE) de 1995. Un dato muy interesante a tener en cuenta es que se ocupa de la exportación de datos personales fuera de la UE.

Si bien la Unión Europea (UE) quiere dar a las personas más control sobre cómo se utilizan sus datos personales, existe también un factor económico que no es menor dado que la UE, podrá ahorrar de esta manera alrededor de 2500 millones de euros ya que será idéntica para todos los Estados que la conforman.

Se adicionan en este GDPR además de los datos de las personas, los llamados identificadores online, como son las direcciones IP, la información cultural, económica o de salud mental.

Se crea entonces a través de este reglamento un marco jurídico que ofrecerá mayor control sobre la

¹Lic. Relaciones Internacionales (UP) 2010. Posgrados en UE-AL (Univ. Bologna, Argentina 2010, 2011, 2012) Posgrado Prevención de lavado de Activos y Financiación del Terrorismo (UBA 2012). Maestría Relaciones Internacionales (UBA). Miembro del Proyecto de Investigación de la Maestría en RR.II UBA 2014-2016. Miembro del Departamento del área de Seguridad y Defensa en IRI, La Plata. Miembro del departamento de Paz y Seguridad en unitedexplanatios.org. Miembro responsable del Depto de Seguridad y Defensa en Zoon-politikon. Fue miembro responsable del Depto de Seguridad y Defensa en Reconciliando Mundos. Miembro investigador en Corte Penal Latinoamericana y del Caribe contra el Crimen Transnacional Organizado (COPLA). Docente y Coordinador de la Maestría en Diplomacia y Política Exterior en UCES sobre Crimen Organizado, Prevención de Lavado de Activos y Financiación del Terrorismo. Expositor y moderador en varios congresos tanto nacionales como internacionales. Cuenta con numerosas publicaciones tanto a nivel nacional como internacional. Fundador de Mente Inter-Nazionale. Mail: mjcorbino@gmail.com



información privada de los y se hará mayor énfasis sobre el nivel de responsabilidad de las empresas en referencia al tratamiento de datos.

Es necesario recordar que hasta el momento que las normas de protección de datos de la UE permiten que los datos personales se puedan procesar solo bajo ciertas condiciones y en determinadas situaciones, por ejemplo, cuando se ha dado el consentimiento explícito o cuando el tratamiento de los datos sea por razones de interés.

El GDPR presenta varios siguientes cambios respecto al tratamiento de datos personales y en cuanto a las multas monetarias que pueden alcanzar según el nivel de infracción hasta los 20 millones de euros, además de la posibilidad de requerir indemnizaciones por parte de los damnificados.

Uno de los puntos que toca el GDPR es el consentimiento reforzado, donde hace referencia a la necesidad de "consentimiento claro y afirmativo" de la persona referente al tratamiento de sus datos personales. A su vez hace referencia al nuevo derecho como el de la "portabilidad" donde permite trasladar los datos a otro proveedor de servicios) y al derecho al "olvido" donde se rectifica o eliminan los datos.

Un punto muy importante a destacar es que las empresas tendrán la obligación de comunicar las filtraciones de seguridad que pudieran provocarse. Debido a esta modificación deberán constantemente monitorear los intentos de intrusión y los accesos no autorizados en sus bases de datos y por ende ser notificados dentro de los plazos establecidos. En referencia a los datos recabados tendrán fines determinados, lo que significa que no será posible utilizarlos con posterioridad con un fin distinto al preestablecido.

Una incorporación clave del GDPR es el Data Protection Officer (DPO) o Delegado de Protección de Datos en castellano. Será utilizada para reforzar y racionalizar la protección de datos para los ciudadanos de la Unión Europea, el GDPR exige el nombramiento obligatorio de un DPO para cualquier organización que procese o almacene grandes cantidades de datos personales, ya sea para empleados, individuos fuera de la organización, o ambos.

Las DPO deben ser "designadas para todas las autoridades públicas, y donde las actividades centrales del controlador o del procesador implican 'el monitoreo regular y sistemático de los sujetos a gran escala' o cuando la entidad lleva a cabo el procesamiento a gran escala de 'categorías especiales de personal data, "' como la que detalla la raza o etnicidad o creencias religiosas. Una de sus funciones será la de identificar los riesgos y buscar las posibles soluciones para solventarlos. Las empresas deberán contar con este delegado, interno o externo, otorgarle total independencia y aportarle las herramientas que necesite cuando las solicite.





**Instituto de
Relaciones
Internacionales**



seguridadydefensa@iri.edu.ar

Es necesario dejar en claro que el DPO será un instrumento voluntario tanto para el responsable como el encargado del tratamiento de datos personales pero que su no designación no exime a las empresas a cumplir con la responsabilidad de realizar un tratamiento correcto de los datos.



Instituto de Relaciones Internacionales

www.iri.edu.ar

Universidad Nacional de La Plata Facultad de Ciencias Jurídicas y Sociales

Calle 48 entre 6 y 7, 5° piso - Edificio de la Reforma - La Plata - Argentina Tel: (54 221) 4230628



Instituto de Relaciones Internacionales - UNLP



@iriunlp

Página 3