Protección de Datos Personales, ¿Responsabilidad de la Empresa?

Alejandro Touriño Peña*

Abogado por la Universidad de Santiago de Compostela.
Máster en Derecho Internacional y Relaciones Internacionales por la Universidad Complutense de Madrid.
Máster en Práctica Jurídica por la Escuela de Práctica Jurídica de la Universidad Complutense de Madrid.
Máster en Derecho de la Propiedad Intelectual e Industrial y en Derecho del Entretenimiento por el IE Law School.

* Esta sección estuvo a cargo de Andrea Mariana Lazo Pérez-Palma, Miembro Asociado de ***ADV EDITORES*** - Revista ***ADVOCATUS***, y Mariana Silva Santisteban López, alumna de octavo ciclo de la Facultad de Derecho de la Universidad de Lima y Directora del Comité Editorial de la Revista.

RESUMEN:

En esta ocasión, ***ADVOCATUS*** tuvo la oportunidad de entrevistar al doctor Alejandro Touriño Peña, líder en el campo del Derecho Europeo de Protección de Datos Personales. A través de las siguientes líneas, se ofrece un análisis del ordenamiento regional de la Unión Europea, medidas de protección ofrecidas, abordando la cuestión desde la óptica de la Responsabilidad Empresarial, culminando en el análisis de un caso práctico.

Palabras Clave: Protección de Datos Personales, Unión Europea, Responsabilidad Civil, Derecho Corporativo.

ABSTRACT:

On this occasion, ***ADVOCATUS*** had the opportunity to interview Alejandro Touriño Peña, leader of the European Personal Data Protection Law field. Throughout the following interview, we offer an analysis of the European Union regional regulations, protection measures offered, addressing the issue from the perspective of Corporate Responsibility, culminating in the analysis of a practical case.

Keywords: Personal Data Protection, European Union, Civil Responsibility, Corporate Law.

1. En su país ¿cómo está regulada la protección de datos personales?

En España, el derecho a la protección de datos es un derecho fundamental que viene reconocido en la Constitución Española y es susceptible de una especial protección.

Igualmente, está regulado el Reglamento del Parlamento Europeo y del Consejo 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 —en adelante, "RGPD"—. El RGPD entró en vigor el 25 de mayo de 2016 y es plenamente aplicable desde el 25 de mayo de 2018.

El RGPD unifica la legislación de protección de datos de los Estados miembros de la Unión Europea y es de aplicación directa. Es decir, no es necesario adoptar un trámite previo de adaptación ni una norma que lo transponga a nivel nacional.

En relación con el ámbito de aplicación territorial, el RGPD resulta aplicable a:

A) Los responsables y encargados del tratamiento que tengan un establecimiento en la Unión Europea, independientemente de que los tratamientos de datos que realice tengan lugar o no, en la misma.

B) Los responsables y encargados del tratamiento que tengan su establecimiento fuera de la Unión Europea y traten datos de personas que se encuentren en la Unión Europea, cuando los tratamientos estén relacionados con la oferta de bienes o servicios a interesados en la Unión Europea o, cuando el tratamiento de datos esté relacionado con el control del comportamiento del interesado en la Unión Europea.

C) Los responsables y encargados no establecidos en la Unión Europea, sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho Internacional Público.

Además, en España existe un proyecto de Ley Orgánica de Protección de Datos que se encuentra en fase de tramitación parlamentaria y cuyo objeto es adaptar al ordenamiento jurídico español, aquellas cuestiones que el RGPD deja al criterio de los Estados miembros. Mientras tanto, sigue siendo aplicable la normativa nacional anterior a la plena aplicación del RGPD, la Ley 15/1999 y su Reglamento de desarrollo, en todos aquellos aspectos que no contradigan al RGPD.

2. Si a un usuario le roban sus datos en su país, ¿qué mecanismos de protección contemplan, con exactitud, las leyes?

En primer lugar, el usuario podrá acudir a la vía administrativa e interponer una reclamación ante la Agencia Española de Protección de Datos —en adelante, "AEPD"—, la Autoridad

de Control con competencia en España para velar por el cumplimiento de la normativa de protección de datos.

En caso de que los datos afectados por el robo sean titularidad de la compañía para la que trabaja el usuario o de la compañía a la que presta servicios, el usuario deberá notificar el robo, de manera inmediata, para que ésta valore si el impacto de la incidencia en la privacidad de los interesados, hace que esta tenga el carácter de brecha de seguridad. En caso de que la incidencia sea tratada como una brecha de seguridad, el responsable del tratamiento deberá notificarla a la AEPD, en un plazo máximo de 72 horas —salvo justificación al respecto— y, en determinados casos, a los usuarios afectados por la violación de seguridad.

Por otra parte, dependiendo de la tipología de datos robados y del uso que terceros no autorizados puedan hacer sobre los mismos, cabe la posibilidad de ejercitar las acciones legales que se detallan a continuación:

a) Interponer una denuncia penal, en caso de que, por ejemplo, se hayan utilizado los datos para suplantar la identidad del usuario.

b) Interponer una demanda por vía civil, si se han vulnerado derechos fundamentales tales como la intimidad, la propia imagen o el honor, teniendo la misma aparejada la reclamación de una indemnización por daños y perjuicios.

A mayor abundamiento, conviene señalar que en caso de que los datos sustraídos estuviesen bajo el control de un responsable o encargado del tratamiento, también cabría la posibilidad de emprender acciones legales contra este —basadas en su falta de diligencia en cuanto a la seguridad y mantenimiento de dichos datos— y denunciarlo a su vez ante la AEPD.

3. ¿Qué medidas se pueden tomar para reducir el impacto del uso indebido de datos?

Dependiendo del impacto de la incidencia y del origen de la misma, el responsable o encargado del tratamiento deberá adoptar medidas técnicas y organizativas apropiadas para evitar que en un futuro se produzca una incidencia similar.

En este sentido y a modo de ejemplo, deberán aplicarse, al menos, medidas que garanticen:

a) La seudonimización y cifrado de los datos;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento y;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

Del mismo modo, la compañía deberá someterse a un proceso de verificación, evaluación y valoración periódico de la eficacia de las medidas técnicas y organizativas adoptadas, a efectos de garantizar la seguridad del tratamiento.

Además, las entidades a las que le resulte de aplicación el RGPD deben cumplir con los principios de protección de datos desde el diseño y por defecto. Es decir, desde la primera fase de desarrollo de un sistema de información o de un nuevo proyecto y durante toda la ejecución del mismo. Esto implicará que, teniendo en cuenta el estado de la técnica, el coste de la aplicación y su naturaleza, ámbito, contexto y fines de tratamiento, así como los correspondientes riesgos de diversa probabilidad y gravedad que entrañe el tratamiento de los derechos y libertades de las personas físicas, el responsable o encargado del tratamiento deberá aplicar medidas técnicas y organizativas apropiadas.

4. ¿Hasta qué punto debería de responsabilizar a las empresas por el mal uso de los datos personales?

Las empresas serán responsables del mal uso de los datos en la medida en la que no hayan adoptado medidas de seguridad, jurídicas y organizativas tendentes a evitar este tipo de incidencias en base al principio de responsabilidad proactiva. Asimismo, recae a su vez en las empresas como responsables o encargadas del

tratamiento el deber de probar el cumplimiento de las obligaciones aplicables recogidas en la normativa.

Es más, las compañías deben dar formación en materia de protección de datos a sus empleados efectos de que estos tengan conocimiento de los procedimientos que deben seguir para dar cumplimiento a la normativa de protección de datos. En caso de incumplimiento por parte del empleado de la normativa de protección de datos, la empresa contratante podrá ejercer contra él las acciones disciplinarias, civiles y/o penales oportunas.

5. En caso de gigantes de la industria, como fue en el caso de la filtración *Cambridge Analytica*, ¿cómo debería aplicarse la protección de datos?

Ante un caso como el de *Cambridge Analytica*, el usuario que tenga conocimiento de la incidencia deberá notificarle de forma inmediata al Delegado de Protección de Datos de la compañía —*Facebook*, por ejemplo—.

Asimismo, el responsable del tratamiento de los datos afectados —*Facebook*, en el supuesto que nos ocupa—, deberá:

a) Comunicar la incidencia a la AEPD sin dilación indebida y en todo caso, antes del transcurso de 72 horas desde su conocimiento, salvo justificación.

b) Notificar la incidencia a los propios interesados cuyos datos se han visto comprometidos, puesto que la brecha supone un riesgo alto para los derechos y libertades de los interesados.

c) Interponer una denuncia ante la AEPD.

d) Aplicar medidas de seguridad técnicas y organizativas para evitar que se produzcan incidencias similares.

e) Registrar la incidencia indicando el origen de la misma, fecha y hora en la que se ha detectado, causas que la han motivado y medidas adoptadas para evitar que se produzcan nuevas incidencias.

Por su parte, el usuario cuyos datos se hayan visto afectados por la brecha de seguridad tendrá derecho a:

a) Interponer una denuncia ante la AEPD.

b) Interponer una demanda por vulneración de su derecho a la intimidad, y, en su caso, honor y propia imagen, teniendo la misma aparejada la reclamación de una indemnización por daños y perjuicios.