La evaluación de riesgos, medida clave en las empresas para cumplir con la nueva normativa de protección de datos

publicado por A. P. el Mié, 08/11/2017

Fundación Inade ha celebrado una nueva sesión de los Diálogos 2020, que ha analizado las nuevas obligaciones de los empresarios según el Reglamento Europeo de Protección de Datos. Para ello se contó con la participación de Marcos López, profesor del Área de Derecho Civil de la UDC, quien aseguró que "la evaluación de riesgos es la medida más importante que deben implementar las empresas para dar cumplimiento a la normativa".

Respecto de los principios aplicables al tratamiento de datos, el profesor indicó que están "establecidos en el artículo 5 del RGPD" y que, "en esencia, se corresponden con aquellos principios que informaban el tratamiento en la LOPD". Estos principios son: de calidad; de consentimiento (antes denominado de licitud); de lealtad; de información (antes, de transparencia); de responsabilidad proactiva (antes, de seguridad); y de secreto.

El principio de calidad, según López, tiene una triple manifestación, ya que "los datos sólo pueden ser objeto de tratamiento para aquella finalidad para la que han sido recabados; deben recabarse los datos que sean estrictamente necesarios; y éstos deben ser veraces y correctos". El segundo ha pasado a pivotar sobre el consentimiento del interesado y establecer unas determinadas excepciones, a tratarse en el RGPD de bases lícitas del consentimiento respecto de las que también se establecen una serie de excepciones que se corresponden con las contenidas en la LOPD. A propósito de este principio, el profesor puso de relieve lo que considera que es una de las características del Reglamento: su inconcreción, afirmando que éste "se halla plagado de conceptos jurídicos indeterminados, así como de remisiones a las futuras legislaciones de los Estados miembros". De la misma manera, el ponente se hace eco de una las críticas del Reglamento: que se haya optado por este instrumento jurídico en lugar de por una Directiva.

Otra cuestión sobre la que llamó la atención López es que, "tanto el Reglamento como la LOPD extienden su ámbito de protección a las personas físicas, lo que planteaba dudas respecto de los datos de profesionales liberales". La Agencia Española de Protección de Datos (AEPD) suplió este vacío legal estableciendo que, si los datos procedían de una relación profesional, quedaban excluidos de la regulación establecida en la LOPD. Sin embargo, como señaló el profesor, "en el Anteproyecto de la que será la nueva Ley de protección de datos, el régimen cambia ya que deja de estar excluido". No obstante, establece que "no es necesario el consentimiento de los interesados". Así, en virtud del principio de licitud, señaló el ponente que "el consentimiento ha de ser inequívoco y será el empresario quien deberá probar que se prestó dicho consentimiento".

El siguiente de los principios objeto de análisis fue el de lealtad, respecto del cual el RGPD no concreta en qué consiste. Sin embargo, por analogía a lo recogido en la LOPD, este deber se concretaría en que los datos deben ser recogidos de manera lícita.

El cuarto de los principios es el relativo a la transparencia, vinculado directamente con el principio de licitud. Este principio obliga al responsable del tratamiento a informar de dónde ha obtenido dichos datos. En cuanto a la forma en que debe practicarse dicha información, hay un contenido mínimo común, con independencia del origen de los datos (aunque, dependiendo del origen, debe facilitarse contenido adicional). Como consecuencia, la información a suministrar puede ser excesiva, por lo que se ha establecido un mecanismo de información por capas, pudiéndose encontrar un modelo en la web de la AEPD.

A continuación, se abordó la explicación relativa al principio de seguridad, del que aclaró que "es una manifestación concreta del principio de responsabilidad proactiva". La aplicación de este principio supone que el responsable del tratamiento de los datos deberá adoptar las medidas de índole técnica y organizativa que sean necesarias para garantizar la seguridad de los datos, evitando en la medida de lo ible su alteración, pérdida, o tratamiento no autorizado. En este aspecto, el ponente puso de relieve diferencias entre el régimen de la LOPD y el del RGPD. "El sistema ha cambiado, de manera que l responsable del tratamiento quien debe analizar los riesgos, dependiendo de la naturaleza de los

datos, para así decidir qué medidas deben implementarse", especificó. Ello se debe a que en el RGPD no existe un elenco tasado de medidas, sino que la lista es de carácter meramente orientativo. Así, será el responsable del tratamiento el que decida qué medidas se van a tomar en función del resultado de la evaluación de riesgos.

El último de los principios analizado fue el relativo a la responsabilidad proactiva, que supone un cambio de paradigma en el sistema de protección de datos. Ello se debe, como apuntó el profesor, a que "se pasa de un procedimiento de protección ex ante a otro que se va a producir ex post". Será la autoridad de control la que, ante denuncia o investigación de oficio, entrará a valorar si se cumplen las medidas necesarias en materia de protección de datos. Así, será el responsable del tratamiento quien decida la aplicación de unas u otras dependiendo de los riesgos asumidos. No obstante, a efectos probatorios, el responsable del tratamiento tiene la posibilidad de acreditar el cumplimiento de los requisitos mediante la adhesión a los códigos de conducta o a través de mecanismos de certificación, a los que sólo se pueden acoger los organismos del sector privado.

Así, el RGPD recoge una serie de medidas que deben ser aplicadas por los responsables del tratamiento de los datos. La primera es una evaluación de riesgos, ya que de esta evaluación se derivan las medidas que se van a aplicar; la segunda es el registro de las actividades del tratamiento, un libro diario donde se recogen los aspectos básicos del tratamiento (debe tenerse en cuenta que con carácter general las empresas de menos de 250 trabajadores están exentas de esta medida). La tercera es la protección desde el diseño y por defecto. Ello quiere decir que, ya desde el principio, se deben adoptar las medidas necesarias para actuar conforme al Reglamento. A continuación, se encuentran las medidas de seguridad. En sexto lugar, las comunicaciones de los fallos de seguridad y, en séptimo y último lugar, la figura del delegado de protección de datos. Marcos López explicó que "los responsables que realicen tratamiento a gran escala, deben designar internamente un delegado que se encargue de supervisar el cumplimiento normativo".

En la segunda parte de la ponencia, referida a los derechos en materia de protección de datos, el profesor hizo especial hincapié en el derecho al olvido (o derecho de supresión, antes de cancelación). Para este derecho, expuso que "el legislador recogió la jurisprudencia emanada por el Tribunal de Justicia de la Unión Europea a propósito del caso Google", especificando, además, la excepción oponible al ejercicio de este derecho, que sería la libertad de expresión e información.

Por último, está el derecho de portabilidad, que faculta al interesado a obtener los datos de un responsable de tratamiento y transmitirlo a otro o, incluso, solicitar que un responsable de tratamiento lo transmita a otro responsable.

Una vez finalizada la presentación del ponente, se abrió un turno de debate en el que se comenzó poniendo de relieve el cambio de paradigma en la protección de datos operado por el RGPD. Así, si antes el empresario tenía claro que cumplía con la legislación con la inscripción de los ficheros, ahora nos encontramos con que esta medida ya no es necesaria, sino que debe elegir qué medidas considera imprescindibles para llevar a cabo una protección adecuada.

También se solicitó del ponente que expresase cuál consideraba que era la medida más importante para dar cumplimiento a la legislación sobre protección de datos, a lo que contestó que "la evaluación de riesgos, sin duda alguna". Ello lo justificó en el hecho de que "de la evaluación de riesgos va a depender directamente la adopción de unas medidas u otras", por lo que la considera fundamental. Esta evaluación será revisable únicamente si hay cambios en el tratamiento de datos, ya que el Reglamento no obliga a una revisión periódica obligatoria.

Otra de las cuestiones suscitadas fue la aplicación de las medidas de seguridad, que según el ponente es "uno de los aspectos claves del RGPD". No obstante, la regulación contenida en el Reglamento, por un lado, da mucha libertad en el establecimiento de estas medidas, pero por otro lado crea inseguridad jurídica al no concretar específicamente qué medidas son exigibles.

Noticias del sector