Expansión | JURÍDICO

Qué cambios deberán asumir las empresas con la nueva LOPD

El texto de la Ley Orgánica de Protección de Datos, que acaba de ser aprobado, plantea nuevas obligaciones que deberán cumplir las compañías, como sucede en relación a las denuncias internas.

TRATAMIENTO

El real-decreto ley 5/2018 concede una moratoria de **4 años** en la firma de contratos de encargo de tratamiento. Los expertos apuestan resolver este asunto antes de 2022.

V. Moreno. Madrid

La nueva Ley Orgánica de Protección de Datos (LOPD) es ya una realidad. Dejando de lado el novedoso Capítulo X, que introduce en nuestro ordenamiento un conjunto de garantías de derechos digitales –derecho al olvido, desconexión digital, neutralidad o la educación digital, entre muchos otros–, y a falta de que el texto sea publicado en el Boletín Oficial del Estado, es importante tener en cuenta los cambios que introduce el texto y cómo afectarán estas novedades en el día a día de las empresas.

María González y Joaquín Cives, responsables de protección de datos de Ecija, creen que todavía quedan muchas incógnitas por resolver en torno al Reglamento General de Protección de Datos (RGPD) –por ser muy general– y a la nueva LOPD. Sin embargo, están convencidos de que es posible extraer ciertos aspectos esenciales que cualquier compañía debería tener en mente para no incumplir sus obligaciones.

Dreamstime

Las sanciones máximas pueden llegar hasta los 20 millones de euros o el 4% de la facturación anual.

Denuncias internas

"El nuevo texto legislativo sobre protección de datos aporta algo de luz frente a las diferentes interpretaciones que hacía la Agencia Española de Protección de Datos (AEPD) y el Grupo de Trabajo del Artículo 29 sobre los canales de denuncias", comenta González. En efecto, la LOPD introduce la posibilidad de que las denuncias puedan ser anónimas y obliga a aplicar importantes medidas de confidencialidad.

La información del *soplón* en el canal de denuncias únicamente se podrá mantener durante un máximo de tres meses. Una vez pasado este tiempo, los datos deberán ser anonimizados y trasladados a otro espacio. En cuanto a la obligatoria comunicación al denunciado, explica la letrada, "ésta podrá ser excepcionada si este intercambio de información pudiera poner en riesgo la culminación de la investigación".

Videovigilancia

La LOPD realiza una actualización de los requisitos en los tratamientos con fines de videovigilancia. Según asegura Cives, hasta el momento sólo existía una instrucción de la AEPD y ahora en el nuevo texto, por fin, se genera una base legitimadora regulada.

Este tratamiento se podrá realizar siempre que la finalidad sea preservar la seguridad de las personas y bienes e instalaciones o control laboral. Las imágenes deberán suprimirse a los 30 días, salvo si se cometen actos contra la seguridad. En este caso, las grabaciones deberán ser puestas a disposición de las fuerzas de seguridad antes de las 72 horas desde el suceso. En caso de la videovigilancia de empleados, éstos siempre deberán tener información previa, expresa, clara y concisa.

Deber de informar

Se lleva a cabo una simplificación de las obligaciones de transparencia e información al afectado. En el sistema de información en dos capas –que adquiere rango normativo–, se reduce el contenido mínimo de la capa básica frente a las recomendaciones de la guía publicada por la AEPD. Además, siempre se deberá indicar una dirección electrónica o medio alternativo para acceder de forma sencilla a la información.

Derecho de acceso

El artículo 13 recoge nuevas especificaciones en el derecho de acceso. De hecho, plantea la posibilidad de que se pueda crear un módulo en el que el titular de los datos pueda acceder a su información de forma remota, directa, simple y segura.

"Según explica el artículo 12.5 del RGPD, en caso de que el interesado repita este ejercicio en menos de seis meses –salvo que exista una causa legítima–, la empresa podrá optar por negarse a atender la solicitud o aplicarle un canon razonable, que la compañía deberá justificar".

Evaluación de impacto

El RGPD impone que, cuando sea probable que un tratamiento implique un alto riesgo para los derechos y libertades de los ciudadanos, el responsable de tratamiento deberá llevar a cabo una evaluación de impacto. "A pesar de lo dicho en la normativa, el RGPD no planteaba supuestos concretos frente a la evaluación de impacto. El nuevo texto de la LOPD, sin embargo, sí que lo hace en su artículo 28", aclara González.

Entre los supuestos en que será obligatorio realizar esta evaluación, hay que destacar cuando se den situaciones de discriminación, usurpación de identidad, fraude, pérdidas financieras o daño para la reputación; la inclusión de datos sensibles o relacionados con la comisión de infracciones administrativas; la transferencia internacional de datos sin el nivel adecuado de protección; así como cuando se trate de personas en situación de vulnerabilidad, como menores de edad o personas con discapacidad.

Régimen sancionador

La LOPD se remite al RGPD en relación al régimen sancionador de las entidades privadas. Éstas van hasta los 10 millones de euros o 2% de la facturación anual o hasta los 20 millones de euros o 4% de la facturación anual, dependiendo de la gravedad de las irregularidades. Sin embargo, no plantea sanciones económicas a las administraciones públicas. La norma también categoriza y plantea los plazos de prescripción de los casos leves –1 año–; graves –2 años– y muy graves –3 años–.

Exclusión publicitaria

"El texto introduce la posibilidad de que cada persona seleccione qué tipo de publicidad quiere recibir", apunta Cives. El letrado realiza esta afirmación puesto que, además de los servicios de exclusiones generales o sectoriales, el nuevo texto de la LOPD añade la posibilidad de incluir sistemas de preferencia para que los ciudadanos limiten la recepción de comunicaciones comerciales de forma personalizada o las procedentes de determinadas empresas.

A efectos de considerar cumplida la obligación por parte de las empresas de consulta previa al envío de publicidad, será suficiente la consulta de los sistemas de exclusión publicados por el órgano de control.

Sesión del Senado de la semana pasada.

¿Qué es y cuándo aplica el interés legítimo?

El interés legítimo es una de las excepciones que existe a la necesidad del consentimiento explícito del interesado. Esta situación permite al responsable tratar datos siempre que, en un ejercicio de ponderación entre el interés legítimo y los derechos fundamentales de la persona, prevalezca el primero sobre los segundos. "Según ha explicado el Grupo Artículo 29, para ser aceptado por la normativa vigente el interés legítimo debe ser concreto, real –y no especulativo– y lícito en relación con el derecho nacional y de la Unión Europea", explica Joaquín Vices, de Ecija. Esta figura, que aparece recogida en el artículo 6 del Reglamento General de Protección de Datos (RGPD) y que no se incluyó en la anterior LOPD, ofrece ventajas y desventajas respecto a la aplicación que se ha hecho hasta ahora. En el primer apartado habría que apuntar que la evaluación que se realiza antes de poder apelar al interés legítimo sirve para identificar los riesgos y a cumplir con el principio de privacidad desde el diseño. Otra ventaja es que el sistema se flexibiliza y que no obliga a colmar al interesado con múltiples solicitudes de consentimiento innecesarias. En la columna de desventajas se encuentran la necesidad de justificar el interés legítimo y el deber de demostrarlo. "Aunque el RGPD no explica cómo realizar este tipo de justificación, lo más adecuado para una empresa es actuar de manera proactiva y documentar el conjunto del proceso de análisis que se realizó antes del inicio del tratamiento", añade María González, 'manager' de protección de datos de Ecija.

La responsabilidad de proteger los derechos de los interesados es mayor, puesto que éstos no han asumido los riesgos al consentir. Lo mismo ocurre con el deber de transparencia, dado que se deben explicar cuáles son los intereses legítimos.