

La nueva Ley Orgánica de Protección de Datos. ¿Qué tengo que hacer?

Isabela Crespo Vitorique

Asociada senior del Área Propiedad Industrial y Tecnologías de la Información de GA_P
Sector de Privacidad y Tecnología

Bárbara Sainz de Vicuña Lapetra

Asociada senior del Área Propiedad Industrial y Tecnologías de la Información de GA_P
Sector de Privacidad y Tecnología

En cumplimiento de la previsión del artículo 99 del Reglamento General de Protección de Datos, ha sido aprobada, pendiente de su publicación, la nueva Ley Orgánica de Protección de Datos que sustituye a la actual concebida como una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar la seguridad jurídica.

La nueva Ley Orgánica de Protección de Datos y de Garantía de los Derechos Digitales (LOPD) ha llegado para quedarse. La LOPD entrará en vigor el día siguiente a su publicación en el Boletín Oficial del Estado con el objeto de completar la adaptación del ordenamiento español al Reglamento General de Protección de Datos (RGPD). La nueva ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales

Corresponde ahora a las entidades comprobar que su actividad es conforme a la nueva norma, de ahí que los principales aspectos o novedades que éstas tendrían que tener en cuenta, en su condición de responsables o encargadas del tratamiento, de acuerdo con lo previsto en la nueva ley orgánica y a modo de decálogo, son los siguientes:

Advertencia legal: Este análisis sólo contiene información general y no se refiere a un supuesto en particular. Su contenido no se puede considerar en ningún caso recomendación o asesoramiento legal sobre cuestión alguna.

N. de la C.: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

1. Garantía de los derechos digitales

Si empezamos por el final, en lo que a ubicación del contenido de la Ley Orgánica de Protección de Datos y de Garantía de los Derechos Digitales se refiere, su gran novedad es el contenido del título X dirigido a los prestadores de la sociedad de la información y a los proveedores de servicios de internet como sujetos encargados de contribuir a garantizar la aplicación de dichos derechos. En el referido título X se acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación derechos y libertades predicables al entorno de internet como la neutralidad de la red y el acceso universal o los derechos a la seguridad y a la educación digital, así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

2. Tratamiento de datos de menores de edad

Si el Reglamento General de Protección de Datos (RGPD) establece como edad mínima los dieciséis (16) años para el tratamiento de datos de menores de edad basado en el consentimiento del propio menor, la ley española, en cumplimiento de la habilitación prevista en el propio reglamento general —según la cual los Estados miembros podrán establecer por ley una edad inferior, siempre que no esté por debajo de los trece (13) años—, fija la edad del menor en catorce (14) años para el tratamiento de datos basado en el consentimiento del menor de edad.

3. Tratamiento de datos personales relativos a condenas e infracciones penales, procedimientos y medidas cautelares y de seguridad conexas

El tratamiento de este tipo de datos para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones o de ejecuciones penales sólo podrá llevarse a cabo cuando se encuentre amparado en una norma de rango legal o en el Derecho de la Unión. En otros supuestos, los tratamientos relativos a tales datos de naturaleza penal sólo podrán llevarse a cabo por parte de abogados y procuradores siempre y cuando tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

4. Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales

El tratamiento de los datos de contacto y, en su caso, los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica se entenderá dentro del interés legítimo perseguido por el responsable del tratamiento o un tercero siempre que se cumplan dos requisitos:

- a) Que se refiera únicamente a los datos necesarios para su localización profesional.
- b) Que la finalidad del tratamiento sea exclusivamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

Lo mismo se presumirá para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales cuando se refieran a tal condición y no se traten para mantener una relación con ellos como personas físicas.

5. Tratamientos relacionados con determinadas operaciones mercantiles

Salvo prueba en contrario, será lícito el tratamiento de datos personales —incluida su comunicación previa— derivado del desarrollo de cualquier operación de modificación estructural de sociedades o de la aportación o transmisión de negocio o de rama de actividad empresarial siempre que sea necesario para el buen fin de la operación y garantice, cuando proceda, la continuación en la prestación de los servicios. Si la operación de que se trate no llega a concluirse, la entidad cesionaria deberá suprimir inmediatamente los datos sin aplicarse la obligación de bloqueo.

6. Tratamientos de datos con fines de videovigilancia

Las personas físicas o jurídicas —públicas o privadas— podrán tratar imágenes mediante un sistema de videovigilancia con la finalidad de preservar la seguridad. En la vía pública sólo podrán captarse imágenes en la medida en que sea imprescindible para la finalidad anterior, no obstante, será posible captar la vía pública en una extensión superior cuando sea necesario para garantizar bienes o instalaciones estratégicas o de infraestructuras vinculadas al transporte. Se prohíbe la captación de imágenes del interior de un domicilio privado y se aclara que el tratamiento por una persona física de imágenes de su propio domicilio queda excluido del ámbito de aplicación de la Ley Orgánica de Protección de Datos y de Garantía de los Derechos Digitales. El plazo máximo de conservación de los datos continúa siendo de treinta días, salvo cuando sea necesaria su conservación para la acreditación de actos contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes serán puestas a disposición de la autoridad competente en el plazo máximo de setenta y dos horas desde el conocimiento de la existencia de la grabación. El responsable del tratamiento debe cumplir el deber de información colocando un dispositivo informativo en un lugar visible donde dé cuenta de la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercer los derechos previstos en el Reglamento General de Protección de Datos, o bien incluyendo en dicho dispositivo un código o enlace a tal información. Por último, la ley orgánica dispone varios requisitos en relación con el uso de los dispositivos de videovigilancia y de grabación de sonidos en el lugar del trabajo:

- Los empleadores podrán tratar las imágenes obtenidas mediante sistemas de videovigilancia para el ejercicio de las funciones de control laboral siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes a él.

- Será necesario informar a los trabajadores acerca de esta medida con carácter previo y de forma expresa, clara y concisa.
- No se permiten los sistemas de videovigilancia y grabación de sonidos en lugares destinados al descanso o esparcimiento tales como vestuarios, aseos, comedores y análogos.
- La utilización de sistemas para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas y siempre respetando los principios de proporcionalidad e intervención mínima y las garantías previstas en la Ley Orgánica de Protección de Datos y de Garantía de los Derechos Digitales.

7. Sistemas de exclusión publicitaria

La Ley Orgánica de Protección de Datos y de Garantía de los Derechos Digitales especifica que será lícito el tratamiento cuyo objeto sea *evitar* el envío de comunicaciones comerciales a quienes se hubiesen opuesto a recibirlas, pudiendo crearse sistemas de información en los que sólo se incluirán los datos imprescindibles para identificar a los afectados. Estos sistemas también podrán incluir servicios de preferencias. Las entidades responsables de los sistemas de exclusión publicitaria deberán comunicar a la autoridad de control su creación, su carácter general o sectorial y el modo en el que los afectados pueden hacer valer sus preferencias. Se impone al responsable la obligación de informar de los sistemas de exclusión existentes a los afectados que manifiesten su negativa a recibir comunicaciones comerciales. Quienes efectúen comunicaciones de mercadotecnia directa deberán consultar previamente los sistemas de exclusión publicitaria y excluir de tal tratamiento los datos de los afectados que hubiesen manifestado su oposición. No será necesario llevar a cabo tal consulta si el afectado hubiera prestado su consentimiento para recibir comunicaciones a quien pretenda realizarlas.

8. Sistemas de información de denuncias internas en el sector privado

La principal novedad en relación con la anterior regulación es que la Ley Orgánica de Protección de Datos y de Garantía de los Derechos Digitales permite que las denuncias puedan ser anónimas. El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes desarrollen las funciones de control interno y de cumplimiento. Se considera lícito acceder a ellos o comunicarlos cuando sea necesario para adoptar medidas disciplinarias o para tramitar procesos judiciales. Sólo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de los recursos humanos. Los responsables del tratamiento deberán adoptar las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, si no lo ha hecho de forma anónima. Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Si fuera necesaria su conservación para continuar la investigación, podrán seguir siendo tratados en un entorno distinto por el órgano de la entidad al que compete dicha investigación. Cuando los datos hayan dejado de ser necesarios, se deberá proceder a su destrucción o eliminación, no siendo aplicable a estos sistemas la obligación de bloqueo.

9. Uso de dispositivos digitales en el ámbito laboral

La Ley Orgánica de Protección de Datos y de Garantía de los Derechos Digitales garantiza el derecho de los trabajadores y empleados públicos a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador. El empleador deberá establecer criterios de utilización de los dispositivos digitales y únicamente podrá acceder a los contenidos derivados de su uso por parte de los trabajadores con el fin de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos. Asimismo, el acceso por el empleador al contenido de dispositivos digitales en uso con fines privados requerirá que se hayan especificado de modo preciso los usos autorizados y se hayan establecido garantías para preservar la intimidad de los trabajadores. En relación con el uso de dispositivos digitales, destaca la incorporación en la ley orgánica del llamado *derecho a la desconexión digital* de trabajadores y empleados públicos con el fin de garantizar el respeto de su tiempo de descanso, permisos y vacaciones, así como el de su intimidad personal y familiar. El empleador deberá definir las modalidades de ejercicio del derecho a la desconexión en una política interna dirigida a los trabajadores donde también se establecerán las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, sujetándose a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

10. Nuevo marco legal

Con la nueva Ley Orgánica de Protección de Datos y de Garantía de los Derechos Digitales quedan derogadas la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la nueva ley orgánica. Sin perjuicio de lo anterior, los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril del 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular por el artículo 22, y por sus disposiciones de desarrollo en tanto no entre en vigor la norma que trasponga al

Derecho español lo dispuesto en la citada directiva. Asimismo, las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad al 25 de mayo del 2018 y, en particular, de los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.