1. Introducción

Anotaciones

El 25 de mayo de 2016 entró en vigor el Reglamento (UE) 2016/679, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos o "RGPD"). Sustituye a la antigua Directiva de protección de datos, que tenía un carácter de mínimos, y permitía a los estados decidir de qué manera cumplir con sus objetivos. El RGPD establece el régimen de protección de datos aplicable a todos los estados de la Unión Europea de manera directa. Sin embargo, otorga un periodo de dos años para que quienes traten datos personales de personas físicas y las agencias de protección de datos se adapten al nuevo sistema, por lo que es de aplicación a partir del 25 de mayo de 2018.

La ya derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal ("LOPD"), y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal ("RLOPD") igualmente derogado; era de las más intuitivas de Europa. Por ello, el nuevo RGPD no introduce tantas diferencias con respecto al régimen anterior como en otros países, si bien siguen existiendo una serie de obligaciones adicionales que deberán cumplirse a partir del 25 de mayo de 2018.

El Consejo de Ministros, a propuesta del ministro de Justicia, Rafael Catalá, ha aprobado el 10 de Noviembre de 2017 el Proyecto de Ley Orgánica de Protección de Datos que adaptará nuestra legislación a las disposiciones del Reglamento (UE) 2016/679 (RGPD), introduciendo novedades y mejoras en la regulación de este derecho fundamental en nuestro país. Uno de los principales objetivos del RGPD es acabar con la fragmentación existente en las distintas normativas de los países comunitarios, esto quiere decir que se pretende unificar los criterios de protección de datos en todos los países miembros de la UE. Además, persigue la adaptación de las normas de protección de datos a la rápida evolución tecnológica y los fenómenos derivados del desarrollo de la sociedad de la información y la globalización.

Nuestro país se caracteriza por ser pionero o postrero en las distintas revoluciones surgidas a lo largo de la Historia. Las nuevas tecnologías no iban a ser una excepción. España fue uno de los primeros países en legislar en la materia. Nuestra Constitución de 1978 ya consignó la palabra *«informática»* en el apartado 4 de su artículo 18, donde dispone que *«la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»*.

Resulta importante poner en valor la gran calidad del texto de nuestra Carta Magna. ¿Cuántos

El 25 de mayo de 2016 entró en vigor el Reglamento (UE) 2016/679, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos o "RGPD"). Sustituye a la antigua Directiva de protección de datos, que tenía un carácter de mínimos, y permitía a los estados decidir de qué manera cumplir con sus objetivos. El RGPD establece el régimen de protección de datos aplicable a todos los estados de la Unión Europea de manera directa. Sin embargo, otorga un periodo de dos años para que quienes traten datos personales de personas físicas y las agencias de protección de datos se adapten al nuevo sistema, por lo que es de aplicación a partir del 25 de mayo de 2018.

La ya derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal ("LOPD"), y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal ("RLOPD") igualmente derogado; era de las más intuitivas de Europa. Por ello, el nuevo RGPD no introduce tantas diferencias con respecto al régimen anterior como en otros países, si bien siguen existiendo una serie de obligaciones adicionales que deberán cumplirse a partir del 25 de mayo de 2018.

Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones, el cual ya viene siendo plenamente aplicable en nuestro país desde el pasado 25.05.18.

ii) Y garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución, regulándose en particular los 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 educación digital así como los derechos al olvido, a la portabilidad y al testamento digital, ocupando 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, resultando también destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

¿Que supone esta nueva ley? Cerrar el círculo de esa nueva era en la regulación de los datos, derogando absolutamente toda la normativa anterior, borrando de un plumazo: la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y el Real Decreto-Ley 5/2018 ya mencionado.

Sin duda, España ha sido pionera en un sistema normativo revolucionario que ahora disfrutamos en toda Europa y que miran con envidia otros países como Estados Unidos, cuyos modelos de negocio *«gratuitos»* se sostienen gracias a una explotación masiva de los datos personales de los usuarios por parte de empresas multimillonarias gracias a una legislación mucho menos protectora de la privacidad de los ciudadanos.

El último hito ha sido la importantísima sentencia del Tribunal de Justicia de la Unión Europea,

de 13 de mayo de 2014, donde se reconoce por vez primera tanto el llamado *«derecho al olvido»* en la Red como, aún más importante, la aplicación de nuestra normativa a los gigantes norteamericanos de Internet como Google o Facebook, cuando traten los datos de europeos. Dicha sentencia fue causada, también, por una acción judicial impulsada desde nuestro país.

El RGPD también persigue aumentar la seguridad jurídica conservando la posibilidad de que el tratamiento de datos se encuentre amparado por una ley, esto quiere decir que el RGPD debe dar prioridad a las medidas destinadas a prevenir las infracciones graves y muy graves, y la mayor parte de estas medidas son jurídicas.

EJEMPLO: Veamos un ejemplo pulsando el siguiente botón. ✱

En el caso de España, la protección de datos es un derecho fundamental protegido por el artículo 18.4 de la Constitución. La protección de datos ocupa un lugar importante dentro del cumplimiento normativo de empresas, autónomos, organismos privados y públicos, entidades, organizaciones, comunidades, etc.... siendo un elemento común y transversal para todos ellos. La normativa actual de protección de datos en España está muy avanzada, no obstante el RGPD introduce ciertas novedades:

- El régimen de consentimiento cambia, a partir de mayo de 2018; desaparecerá el consentimiento tácito o por omisión, que implicaba que los datos serían usados salvo que se manifestase la negativa de forma expresa y, en cambio, se exige una acción "afirmativa y expresa" por parte del afectado.
- Se introducen nuevas figuras como por ejemplo el Delegado de Protección de Datos, que tendrá que existir en determinados casos. El delegado es una persona física o jurídica y los encargados de nombrar al Delegado de Protección de Datos serán los responsables de ficheros o encargados del tratamiento.
- Ese nombramiento deberá comunicarse a la Agencia Española de Protección de Datos al ser la autoridad encargada del control del cumplimiento de la legislación sobre Protección de Datos.
- También se comunicará a los afectados ya que tienen derecho a acudir ante el Delegado de Protección de Datos si consideran que se han vulnerado sus derechos o para realizar cualquier consulta sobre la materia. se analiza esta figura detenidamente en el presente curso.
- Adelanta a los 13 años la edad de consentimiento para el tratamiento de datos en consonancia con la normativa de otros países.
- Se tomará en cuenta el tratamiento de los datos correspondientes a personas fallecidas en base a la solicitud de sus herederos , es decir se permitirá a los herederos solicitar el acceso a datos de sus personas fallecidas, así como su rectificación o supresión.
- Se excluye la figura del consentimiento tácito que se sustituye por una acción afirmativa y expresa por parte del afectado como se verá a lo largo del curso.

Se recoge manifiestamente el deber de confidencialidad, esto es, este deber de secreto o confidencialidad comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el 'deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

EJEMPLO: Veamos un ejemplo pulsando el siguiente botón. ✱

En caso de inexactitud en los datos personales obtenidos de forma directa, se excluye la imputabilidad del responsable de su tratamiento si éste ha adoptado todas las medidas razonables para su rectificación o supresión. Los datos deben ser exactos y puestos al día de modo que respondan con veracidad a la situación actual del afectado. Es decir, se exige al responsable del tratamiento que actúe con la diligencia necesaria, con el fin de asegurar, en la medida de lo razonable, que los datos que trata son correctos, completos, y que están debidamente actualizados. Según el artículo 16 del RGPD si la persona detecta que sus datos contienen alguna inexactitud, puede solicitar que se rectifiquen, petición que debe atenderse por parte del responsable en el plazo de un mes.

EJEMPLO: Veamos un ejemplo pulsando el siguiente botón. ✱

En las cuestiones relacionadas con el tratamiento de datos, incorpora el principio de transparencia en cuanto al derecho de los afectados a ser informados sobre dicho tratamiento. Derecho del interesado y por ende obligación del responsable del tratamiento, a recibir/proporcionar toda información y comunicación relativa al tratamiento de datos de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, y, además, en su caso, que se visualice.

Contempla de forma expresa los derechos de acceso, rectificación, supresión, derecho a la limitación del tratamiento, así como a la portabilidad y oposición, incorporando por tanto nuevos derechos para los afectados. Igualmente se tratan los derechos en el presente curso.

Para evitar situaciones discriminatorias, se mantiene la prohibición de almacenar datos de especial protección, como ideología, afiliación sindical, religión, orientación sexual, origen racial o étnico y creencias. En estas categorías, el solo consentimiento del interesado no basta para dar viabilidad al tratamiento; Los Responsables o Encargados que realicen tratamientos de categorías especiales de datos deberán atenerse a las siguientes obligaciones específicas que dispone el Reglamento:

- Elaboración de perfiles (artículo 22, apartado 4)
- Registro de actividades (artículo 30, apartado 5)
- Evaluación de impacto (artículo 35, apartado 3.b)

- Delegado de protección de datos, DPO (artículo 37, apartado 1.c)

Otra novedad importante es que introduce algunos supuestos en los que el legislador contempla como presunción, la prevalencia del interés legítimo del responsable del tratamiento de los datos en cumplimiento de determinados requisitos, como en el caso de los sistemas de información crediticia. Es decir, por lo que respecta al suministro de información crediticia se establece una serie de restricciones respecto de los ficheros de solvencia patrimonial, exigiendo el consentimiento del interesado, salvo que los datos procedan de fuente accesible al público y a la vez para que el tratamiento de datos relativos a obligaciones financieras o de crédito se consideren lícitos deben concurrir una serie de requisitos:

- Datos facilitados por el acreedor.
- Datos referidos a deudas ciertas, vencidas y exigibles y no reclamadas.
- El acreedor debe informar al afectado sobre de la posibilidad de inclusión en dichos sistemas.
- El acreedor haya requerido previamente de pago al deudor.

La entidad de información crediticia notificará al afectado la inclusión de sus datos y le facilitará el ejercicio de los derechos de acceso, rectificación o supresión dentro de los 30 días siguientes a la inclusión de la deuda. Durante este plazo los datos estarán bloqueados.

Se regulan las situaciones en las que se aprecia la existencia de interés público, como los relacionados con la videovigilancia y sistemas de exclusión publicitaria (listas Robinson), la función estadística pública y las denuncias internas en el sector privado.

EJEMPLO: Veamos un ejemplo pulsando el siguiente botón. ✱

Importancia de los datos personales entre países

Autoridad

El régimen de consentimiento cambia, a partir de mayo de 2018; desaparecerá el consentimiento _____ o por omisión, que implicaba que los datos serían usados salvo que se manifestase la negativa de forma expresa y, en cambio, se exige una acción "afirmativa y expresa" por parte del afectado.

- Tácito
- Expreso

Se recoge manifiestamente el deber de confidencialidad, esto es, este deber de secreto o confidencialidad comporta que el responsable de los datos almacenados no pueda revelar ni