

TALLER de la FDE en el CONGRESO de DERECHO SANITARIO

I) ANTEPROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

(D. José Amerego Alonso – Secretario General Técnico del Ministerio de Justicia)

1. Antecedentes

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución.

El último hito en la evolución en materia de protección de datos ha tenido lugar con la adopción del **Reglamento (UE) 2016/679 del Parlamento Europeo y del 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 (**Reglamento General de Protección de Datos**).

Este Reglamento General de Protección de Datos implementa un nuevo modelo basado en lo que se denomina “**enfoque de riesgo**” o de “**responsabilidad activa**”, consistente en la necesaria *evaluación por los propios responsables y encargados del tratamiento de los riesgos que su actividad puede generar en el derecho fundamental para, a partir de esa valoración, adoptar las medidas que resulten necesarias* para mitigarlos en todo lo que sea posible.

Es decir, que en adelante se exigirá al sujeto obligado por la norma (responsable y encargado del tratamiento de datos) la adopción de medidas tales como la realización de evaluaciones de impacto en la protección de datos o la implantación de medidas de seguridad técnicas y organizativas ajustadas en cada momento al estado de la técnica y a los riesgos derivados del tratamiento.

La aplicación del nuevo reglamento europeo a partir del 25 de mayo de 2018 plantea la necesidad de adaptar el ordenamiento jurídico español para que dicho reglamento pueda desplegar sus efectos, por lo que desde el Ministerio de Justicia se aprobó impulsar el anteproyecto de Ley Orgánica de Protección de Datos, actualmente en tramitación.

2. Anteproyecto de la Ley Orgánica de Protección de Datos:

Dado que el Reglamento General de Protección de Datos es una norma directamente aplicable, no precisa incorporación mediante otra de naturaleza interna, si bien ello no es óbice para que existan otras normas internas que complementen su contenido. En este sentido, el RGPD incorpora más de 50 llamamientos al legislador que permitan su "desarrollo" y adaptación a las normativas internas de los Estados Miembros.

En consecuencia, el anteproyecto de Ley Orgánica de Protección de Datos (“*anteproyecto de la LOPD*”) está llamado a preservar la seguridad jurídica, pues proporciona un nuevo marco acomodado al Reglamento General de Protección de Datos al tiempo que deroga la vigente legislación orgánica.

A estos efectos es importante recalcar que el estudio de la normativa de protección de datos exigirá el próximo año la consulta simultánea de dos textos, uno europeo - directamente aplicable- y otro nacional, que complementa el anterior. Precisamente para facilitar esta convivencia, el anteproyecto sigue una ordenación similar a la del Reglamento General de Protección de Datos.

3. Novedades introducidas por el anteproyecto de LOPD

En cuanto al anteproyecto de LOPD procede resaltar la importancia que se da a los **datos relativos a la salud**, categoría en la que, conforme al considerando trigésimo quinto del Reglamento General de protección de Datos, “*se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro*”. Así, tales datos comprenden:

- La información sobre la persona física recogida con ocasión de su inscripción a efectos de *asistencia sanitaria*, o con ocasión de la prestación de tal asistencia (...).
- *Todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios.*
- *Toda información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal*, incluida la procedente de datos genéticos y muestras biológicas.
- *Cualquier información relativa, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado*, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro”.

En la norma europea los **datos relativos a la salud** tienen la consideración de **datos especialmente protegidos**, en los términos del artículo 9.1, conforme al cual su tratamiento queda prohibido, salvo que concurra alguna de las circunstancias mencionadas en el apartado 2 del mismo precepto, entre ellas:

- Que el interesado haya dado su **consentimiento explícito** para el tratamiento de dichos datos personales, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición no puede ser levantada por el interesado;
- Que el **tratamiento sea necesario para proteger intereses vitales del interesado** o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

- Que el *tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social*, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario;
- Que el *tratamiento sea necesario por razones de interés público* en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

Por su parte, el anteproyecto de Ley Orgánica de Protección de Datos preserva la importancia de los datos relativos a la (especialmente protegidos), *sin impedir su tratamiento en el caso de que concurra el consentimiento explícito del afectado*. Con este fin se prevé la posibilidad de que la ley ampare el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

En el marco del principio de **responsabilidad activa**, corresponde a *los responsables y encargados de tratamiento de datos* ponderar los riesgos que el tratamiento pueda generar en los derechos de los afectados y en particular en su derecho a la protección de datos, a la hora de determinar las medidas técnicas y organizativas apropiadas que deben aplicar. Para la adopción de tales medidas, se habrán de tener en cuenta los riesgos que entrañan la creación y utilización de perfiles personales mediante el análisis de aspectos referidos a su salud.

Finalmente, el anteproyecto ha especificado qué entidades, en todo caso, **han de designar un delegado de protección de datos**, incluyendo los **centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes** con arreglo a lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Supone ello que tales centros han de contar con una figura que, sea una persona física o jurídica, esté o no integrada en la plantilla de la entidad, participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

II) NUEVO MODELO DE PROTECCIÓN DE DATOS SANITARIOS

(D. Jose Luis Piñar Mañas – Catedrático de derecho Administrativo)

Como indicábamos anteriormente, el nuevo modelo de Protección de Datos de carácter personal parte del principio de “*responsabilidad activa*”, de modo que corresponde a los responsables y encargados de tratamiento de datos ponderar los riesgos que el tratamiento pueda generar a la hora de determinar las medidas técnicas y organizativas apropiadas que deben aplicar.

Entre algunas de las restantes novedades, podemos destacar las siguientes:

- Privacidad desde el diseño
- Fin de la obligación de inscripción de los ficheros
- Evaluación de impacto y Consulta Previa a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.
- Obligación del responsable del tratamiento de notificar a la autoridad de control competente cualquier violación de la seguridad de los datos personales, sin dilación indebida y a más tardar 72 horas después de que haya tenido constancia de la misma.
- Las sanciones en caso de incumplimiento se impondrán al “responsable y/o al encargado del tratamiento de datos”, no al Delegado de Protección de Datos.
- Posibilidad de los interesados de presentar reclamaciones ante las autoridades de control del Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la comisión de la supuesta infracción
- Incremento de las sanciones hasta 20 000 000 EUR o, tratándose de una empresa, cuantía equivalente al 4 % del volumen de negocio total anual global.

III) RÉGIMEN DE LOS DATOS DE SALUD EN EL RGPD

[D. Miguel Geijo Castany – Secretario de la Asociación de Profesionales Españoles de Privacidad (APEP)]

Destacar la gran inseguridad jurídica que se ha generado con el nuevo RGPD a causa del principio de “*responsabilidad activa*”.

I) REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL 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 (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS).

[D^a. Mar España Martí – Directora de la AEPD]

1. Impacto del RGPD en las Organizaciones Colegiales:

En España existen más de 1.300.000 profesionales colegiados de los cuales unos 700.000 pertenecen al sector salud. A este respecto, en el RGPD los datos relativos a la salud tienen la consideración de datos especialmente protegidos.

A pesar de esta importancia en cuanto al tratamiento de esta categoría de datos, conforme a los datos de la AEPD, hasta la fecha únicamente un 2,5% de los procedimientos sancionadores de la Agencia han afectado al sector salud, y únicamente en un 0,27% de los casos se han impuesto sanciones económicas.

A efectos de procurar mantener estas buenas cifras en cuanto al tratamiento de los datos Sanitarios, en aquellos casos en los que se produzca algún tipo de vulneración en materia de Protección de Datos por parte de los profesionales sanitarios, las primeras medidas que prevé adoptar la AEPD son los apercibimientos y no las sanciones pecuniarias.

En este sentido, la AEPD modifica la posición “*reactiva*” que venía manteniendo hasta la fecha, consistente en sancionar aquellas vulneraciones en materia de tratamiento de datos personales, y adopta en su lugar una posición “*preventiva*” consistente en concienciar a los responsables y encargados de protección de datos sobre la necesidad de tratar los datos personales con diligencia.

Sin embargo, no hay que perder de vista que el nuevo modelo instaurado pro el RGPD parte del principio de “**responsabilidad activa**”, correspondiendo al responsable del tratamiento de datos (y al encargado, en su caso) justificar que las medidas de tratamiento de datos adoptadas eran suficientes teniendo en cuenta la categoría y sensibilidad de los datos que manejan. Así pues, y si bien es cierto que se da una mayor flexibilidad a los responsables del tratamiento de datos, ello genera, a su vez, una gran inseguridad jurídica.

Por esta razón la AEPD recaba la colaboración de las Organizaciones Colegiales y, especialmente, de sus Consejos Generales, a fin de conocer las particularidades de los destinos sectores y resolver en la medida de lo posible todas las dudas que puedan surgir

en cuanto a la aplicación del nuevo RGPD así como de cara a elaborar modelos de “análisis de riesgo” o de “clausulas informativas” adaptadas a las necesidades del sector.

Se contempla, además, la creación de un listado de Delegados de Protección de Datos y la publicación pro parte de la agencia de una serie de guías que faciliten la tarea de adaptarse a la nueva legislación en materia de Protección de Datos.

Se requiere, en definitiva, por parte de la AEPD la colaboración de las organizaciones Colegiales y su implicación a fin de facilitar el tránsito a esta nueva legislación.