LAW-FAQ
o
CATECISMO JURÍDICO PARA INFORMÁTICOS
2. PROTECCIÓN DE DATOS

José Luis Pérez de la Cruz
Licenciado en Derecho
Catedrático de Lenguajes y Ciencias de la Computación
de la Universidad de Málaga

22 de mayo de 2018

Compuesto por el autor mediante LaTeX

1. Conceptos generales

¿Qué conflictos regula el Derecho de protección de datos?

Los que surgen entre los intereses de quienes desean recopilar, almacenar, procesar y usar datos relativos a personas físicas y el derecho de éstas a controlar el uso y destino que se haga de estos datos.

La Constitución española garantiza el derecho a la intimidad personal y familiar y preceptúa que para ello la ley limitará el uso de la informática[1]. El Tribunal Constitucional estableció que esta limitación del uso de la informática constituye un derecho fundamental diferente al derecho a la intimidad, al que podría denominarse "derecho a la libertad informática" o "derecho a la autodeterminación informativa"[2].

¿Es lo mismo "intimidad" que "privacidad"?

"Intimidad" es una palabra que siempre se ha empleado en el Derecho español. La palabra equivalente en inglés es "privacy" y para traducirla algunos recurren al neologismo "privacidad". Se ha propuesto aprovechar esta nueva palabra para referirse con ella al "derecho a la autodeterminación informativa" antes mencionado.

¿Qué leyes regulan en España el Derecho de protección de datos?

A partir del 25 de mayo de 2018 es aplicable el *Reglamento General de Protección de Datos* (RGPD) publicado por la Unión Europea en mayo de 2016[3]. En este momento se está debatiendo en el Congreso de los Diputados una nueva Ley Orgánica de Protección de Datos de Carácter Personal que sustituya a la hasta ahora vigente LOPD[4] y concrete los puntos que la norma europea no considera, o bien remite a las legislaciones nacionales.

¿Existe algún órgano encargado de hacer cumplir esas normas?

Sí, la Agencia Española de Protección de Datos (AEPD), que es la *Autoridad de control* en la terminología del RGPD.

¿Es la AEPD quien en última instancia interpreta y aplica el Derecho de protección de datos?

No; son los tribunales y, en particular, la Audiencia Nacional, ante la cual pueden recurrirse las resoluciones de la AEPD[5].

¿Y vale la pena recurrir las resoluciones de la AEPD?

Depende. La Audiencia anula a veces las resoluciones de la AEPD, pero el proceso es costoso y el resultado en general impredecible[6].

¿Qué sanciones puede imponer la AEPD a quienes no cumplan las normas?

[1] Art. 18 de la Constitución.

[2] Sentencia del Tribunal Constitucional 292/2000.

[3] 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 datos personales y a la libre circulación de estos datos.

[4] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[5] Disposición adicional cuarta, apartado 5, de la Ley 29/1998 reguladora de la Jurisdicción Contencioso-Administrativa.

[6] En 2012, según la Memoria de la AEPD, la Audiencia Nacional estimó íntegramente el 22 % de los recursos presentados contra las resoluciones de la Agencia.

Multas, que según el RGPD pueden ser de hasta 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior[7].

También puede imponer una limitación temporal o definitiva del tratamiento de datos, e incluso prohibirlo; y ordenar la rectificación o supresión de datos personales[8].

¿Puede la AEPD ordenar que se pague una compensación a una persona lesionada en sus derechos?

No. Las multas impuestas por la AEPD tienen el carácter de sanción administrativa y su importe no pasa al patrimonio del interesado, sino al Tesoro Público.

Si el interesado quiere obtener el resarcimiento de los daños y perjuicios causados por un particular, deberá presentar la correspondiente demanda ante los tribunales ordinarios (jurisdicción civil). Si los daños los causó un organismo público, deberá exigir la responsabilidad patrimonial de la Administración ante los correspondientes órganos administrativos o recurrir a la jurisdicción contencioso-administrativa.

¿Puede la AEPD condenar a penas de cárcel a quienes infrinjan los preceptos de la LOPD?

¡Por supuesto que no! La AEPD es un órgano administrativo. Sólo los jueces y tribunales del orden penal pueden hacerlo, y sólo para las conductas descritas en el Código Penal.

¿Y qué conductas relativas a los datos personales están descritas en el Código Penal?

En él se establece que será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses:

—El que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

—El que, sin estar autorizado, acceda por cualquier medio a los mismos y el que los altere o utilice en perjuicio del titular de los datos o de un tercero.

Estas penas se ven agravadas en ciertos casos, por ejemplo, cuando se trata de datos que revelan la ideología, religión, creencias, salud, origen racial o vida sexual; o cuando los hechos los realiza una autoridad o funcionario público prevaliéndose de su cargo[9].

¿Dónde se puede encontrar más información práctica acerca del Derecho de protección de datos?

En el sitio web de la AEPD (`www.agpd.es`) hay abundante información.

2. Tratamiento de datos

¿Qué datos se consideran* personales*?

[7] Art. 83 RGPD.
[8] Art. 58 RGPD.
[9] Arts . 197 y 198 del Código Penal.

Se entiende por "datos personales" toda información sobre una persona física identificada o identificable. Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona[10].

Esta persona física se denomina *el interesado*.

¿Son las direcciones de correo electrónico datos personales?

En la práctica sí, según el criterio de la AEPD y los Tribunales.

¿Y las direcciones IP?

Sí, según criterio constante de los Tribunales europeos y españoles[11].

¿Son las* imágenes *datos personales?

Sí, según criterio constante de la AEPD y de la Audiencia Nacional.

¿Qué legislación es aplicable si las imágenes se captan en lugares públicos?

En los lugares públicos únicamente están legitimadas para la captación de imágenes las Fuerzas y Cuerpos de Seguridad del Estado, en los términos de su legislación específica[12].

¿Pueden los particulares instalar sistemas de videovigilancia?

Sí. Los ficheros se rigen por la Instrucción que la AEPD ha dictado para regular estos sistemas[13] :

—Los particulares no pueden instalar sistemas de grabación en lugares públicos más allá de lo que resulte idóneo, adecuado y proporcional a sus lícitas finalidades.

—Sólo se considerará admisible la instalación de cámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

—El deber de información exige colocar en las zonas videovigiladas un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados.

—Los datos se cancelarán en el plazo máximo de un mes.

¿Qué se entiende por* tratamiento *de datos?

Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por

[10] Art. 4 RLOPD.

[11] vd. sentencia de la Audiencia Nacional de 1 septiembre 2011.

[12] Ley Orgánica 4/1997, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos

[13] Instrucción 1/2006, de la AEPD en materia de videovigilancia.

transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción[14].

Nótese que la mera recogida de los datos ya constituye un "tratamiento" de los mismos.

¿Cuáles son las categorías especiales *de datos personales?*

Los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. El tratamiento de estos datos está sometido a restricciones adicionales[15].

¿Qué se entiende por seudonimización*?*

El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable[16].

¿Qué se entiende por fichero*?*

Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica[17].

El RGPD se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero[18]. Es decir, la protección afecta en particular a los datos informatizados, pero también a los que tienen como soporte el papel o cualquier otro medio.

¿Afectan las disposiciones del RGPD a todos los tratamientos de datos?

No. El Reglamento no se aplica al tratamiento de datos personales:

—efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

— o por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención[19].

¿Qué entiende el RGPD por responsable *o* responsable del tratamiento*?*

[14] Art. 4 RGPD.
[15] Art. 9 RGPD.
[16] Art. 4 RGPD.
[17] Art. 4 RGPD.
[18] Art. 2 RGPD.
[19] Art. 2 RGPD.

La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento[20].

¿Qué entiende el RGPD por* encargado *del tratamiento?

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento[21].

3. Principios del tratamiento

¿A qué obliga el principio de* limitación de la finalidad *de los datos?

Los datos serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

El tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales[22].

¿A qué obliga el principio de* minimización *de los datos?

Los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados[23].

¿A qué obliga el principio de* exactitud *de los datos?

Los datos serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan[24].

¿A qué obliga el principio de* limitación del plazo de conservación *de los datos?

Los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento. Podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos[25].

¿A qué obliga el principio de* integridad y confidencialidad *de los datos?

Los datos serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas[26].

[20] Art. 4 RGPD.
[21] Art. 4 RGPD.
[22] Art. 5.1 RGPD.
[23] Art. 5.1 RGPD.
[24] Art. 5.1 RGPD.
[25] Art. 5 RGPD.
[26] Art. 5.1 RGPD.

¿En qué consiste el principio de* responsabilidad proactiva *del responsable?

El responsable del tratamiento será responsable del cumplimiento de todos los principios anteriores y debe ser capaz de demostrarlo[27].

¿Cuál es la condición necesaria para que el tratamiento sea lícito?

El tratamiento solo será lícito, salvo excepciones, si el interesado dio su consentimiento para el tratamiento de sus datos para uno o varios fines específicos[28].

¿Qué se entiende por* consentimiento*?

Es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen[29].

El responsable deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales[30].

Nótese que se exige una declaración o una "acción afirmativa"; el consentimiento no se supone, ni puede ser tácito.

¿Da el RGPD algunas indicaciones sobre cómo redactar la solicitud de consentimiento?

Sí. Si el consentimiento se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.

Además, para evaluar si el consentimiento se ha dado libremente se tendrá en cuenta el hecho de si, entre otras cosas, la ejecución de un contrato se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato[31].

¿Se puede solicitar el consentimiento vía formulario web?

Sí. Cuando la recogida de datos se efectúa en una página web, el deber de información puede cumplirse mediante formularios y cláusulas a los que se accede a través de enlaces titulados, por ejemplo, "aviso legal" o "política de protección".

Para asegurar que el consentimiento sea específico e informado, hasta que el interesado acceda a las advertencias anteriores debe resultar imposible la introducción de dato alguno en la página.

¿Cómo ha de ser el consentimiento para el tratamiento de categorías especiales de datos?

Debe ser explícito y para un fin determinado. La UE y los Estados podrán establecer casos en los que el tratamiento sea ilícito, incluso mediando el consentimiento del interesado[32].

[27] Art. 5.2 RGPD.
[28] Art. 6.1 RGPD.
[29] Art. 4.11 RGPD
[30] Art. 7.1 RGPD
[31] Art. 7.2 y 4 RGPD
[32] Art. 9 RGPD

¿Se puede revocar el consentimiento?

El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo[33].

¿Cuál es la edad mínima para prestar el consentimiento al tratamiento de datos personales?

El RGPD establece los 16 años, aunque permite que cada Estado la fije entre 13 y 16 años[34]. La legislación española fijaba los 14 años.

¿Cuáles son las excepciones a la necesidad del consentimiento?

Entre otras son:

—Que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

—Que el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

—Que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física.

—Que el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

—Que el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado[35].

4. Derechos del interesado

¿En qué consiste el derecho de acceso*?*

El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen[36]. Si es así, tiene derecho a acceder a tales datos personales y a ser informado sobre el uso que se les da.

El responsable facilitará una copia de los datos personales objeto de tratamiento[37].

¿En qué consiste el derecho de rectificación*?*

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos[38].

¿En qué consiste el derecho de supresión*?*

El interesado tendrá derecho que el responsable del tratamiento suprima los datos personales que le conciernan cuando concurra alguna de las circunstancias siguientes:

[33] Art. 7.3 RGPD.
[34] Art. 8.1 RGPD.
[35] Art. 6.1 RGPD.
[36] Art. 15.1 RGPD.
[37] Art. 15.3 RGPD.
[38] Art. 16.1 RGPD.

—los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

—el interesado retire el consentimiento en que se basa el tratamiento;

—los datos personales hayan sido tratados ilícitamente[39].

¿Qué se entiende por elaboración de un perfil*?*

Es toda forma de tratamiento automatizado de datos personales consistente en utilizarlos para evaluar determinados aspectos de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos[40].

¿En qué consiste el derecho de oposición*?*

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de tratamiento, incluida la elaboración de perfiles.

El responsable dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado.

Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia[41].

¿Qué derechos tiene el interesado respecto a sus perfiles?

Como ya hemos dicho, puede oponerse a que se elaboren.

Además, el interesado tendrá derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar[42].

¿En qué consiste el llamado "derecho al olvido"?

La carga de boletines oficiales y otras fuentes de datos en la web y su posterior indexación por los buscadores permiten el acceso instantáneo y cómodo, por parte de cualquier persona y desde cualquier lugar, a datos que anteriormente sólo podían encontrarse, si acaso, después de desplazarse físicamente a una biblioteca y realizar un considerable esfuerzo de búsqueda. Esto tiene muchas ventajas para los investigadores, pero puede también dar lugar a situaciones inconvenientes: ciertos datos molestos (multas, condenas, noticias embarazosas aparecidas en la prensa) están ahora al alcance inmediato de cualquier curioso. El derecho al olvido consiste en la facultad del interesado para oponerse a la indexación de estos datos personales por los buscadores web, aun cuando sean veraces y hayan aparecido en fuentes públicas. Este derecho al olvido es una manifestación del derecho de supresión o de oposición.

[39] Art. 17.1 RGPD.
[40] Art. 4 RGPD.
[41] Art. 21 RGPD.
[42] Art. 22 RGPD.

¿Reconoce la ley el derecho al olvido?

El Tribunal de Justicia de la Unión Europea (TJUE) dictó sentencia en el "caso Mario Costeja"[43] en la que se reconoce este derecho.

¿En qué consiste el* derecho de limitación*?

El interesado tendrá derecho a obtener del responsable la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado[44].

¿En qué consiste el* derecho de portabilidad*?

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado. Al ejercer este derecho, el interesado podrá exigir que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible[45].

5. Deberes del responsable y del encargado

El responsable, ¿está obligado a facilitar al interesado alguna información cuando le solicite sus datos?

Sí. Deberá proporcionar la siguiente información:

1.a) la identidad y los datos de contacto del responsable o su representante;

1.b) los datos de contacto del delegado de protección de datos, si lo hay;

1.c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

1.e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

1.f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional;

2.a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

2.b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

[43] Sent. TJUE de 13 de mayo de 2014 en el asunto C-131/12.
[44] Art. 18 RGPD.
[45] Art. 20 RGPD.

2.c) la existencia del derecho a retirar el consentimiento en cualquier momento;

2.d) el derecho a presentar una reclamación ante una autoridad de control;

2.e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato;

2.f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles y, a menos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado[46].

¿Y si los datos no se han obtenido directamente del interesado?

Deberá proporcionarle además información acerca de la fuente de que proceden los datos, y si proceden de fuentes de acceso público[47].

Eso es mucha información. ¿Cómo se puede proporcionar de forma comprensible?

La AEPD ha elaborado una "Guía para el cumplimiento del deber de informar" (`www.agpd.es`) donde se proporcionan algunas indicaciones para ello. La AEPD recomienda estructurar la información en dos niveles, el básico y el adicional. El básico se muestra directamente al interesado y el adicional es accesible fácilmente, normalmente mediante un hipervínculo o URL. La fig. 1 muestra un ejemplo para un caso ficticio de suscripción a una revista, tomado de dicha "Guía".

Información básica sobre Protección de Datos	
Responsable	Ediciones Warren&Brandeis, S.A. +info...
Finalidad	Gestionar el envío de información y prospección comercial +info...
Legitimación	Consentimiento del interesado +info...
Destinatarios	Otras empresas del grupo Warren&Brandeis, Inc. Encargados de Tratamiento fuera de la UE, acogido a "Privacy Shield" +info...
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional +info...
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: http://www.warrenbrandeis.com/protecciondatos/info/

Figura 1: Deber de informar (tomado de [1])

¿Hay algún caso en que no sea obligatorio proporcionar esta información?

Sí. El responsable no está obligado a facilitar ninguna información

[46] Art. 13 RGPD.
[47] Art. 14.1 y 2 RGPD.

—si el interesado ya dispone de ella;

—si la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos[48].

¿Quién está obligado a llevar un registro de actividades de tratamiento*?*

El responsable debe llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

El encargado debe llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable.

Esta obligación se aplica a toda empresa u organización que cumpla alguna de las siguientes condiciones:

—que el tratamiento no sea ocasional;

—que emplee a 250 personas o más;

—que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados;

—que el tratamiento incluya categorías especiales de datos personales, o datos personales relativos a condenas e infracciones penales[49].

¿Qué debe contener el registro de actividades de tratamiento?

El contenido se detalla en el art. 30 del RGPD. Recomendamos al lector que consulte el registro de la AEPD, que lo ha publicado en su página web, y que estudie la documentación generada por el programa *Facilita* de la AEPD.

¿Qué se entiende por violación de la seguridad de los datos*?*

Es toda destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos[50].

¿Qué debe hacer el responsable en caso de violación de seguridad?

La notificará a la autoridad de control (AEPD) sin dilación indebida, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación[51].

También la documentará, incluyendo los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas[52].

Además, cuando sea probable que la violación de la seguridad entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida[53]. No obstante, si los datos estaban cifrados, no es necesaria la comunicación al interesado, ni

[48] Art. 14.4 RGPD.
[49] Art. 30 RGPD.
[50] Art. 4 RGPD.
[51] Art. 33.1 RGPD.
[52] Art. 33.5 RGPD.
[53] Art. 34.1 RGPD.

tampoco si el responsable ha tomado medidas ulteriores que garanticen que el riesgo no se concretará. Por otra parte, si la comunicación individual supone un esfuerzo desproporcionado, se puede optar en su lugar por una comunicación pública o una medida semejante[54].

¿Qué debe hacer el encargado en caso de violación de seguridad?

El encargado del tratamiento notificará sin dilación indebida al responsable las violaciones de la seguridad de los datos personales de las que tenga conocimiento[55].

¿Cuál es el principal deber del responsable del tratamiento?

Es la *seguridad* del tratamiento. El responsable debe aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas[56]

En particular, deberá aplicar los principios de

—*Protección de datos desde el diseño* del sistema de información. Desde el momento de determinar los medios de tratamiento se han de prever las medidas técnicas y organizativas apropiadas para cumplir lo dispuesto en el RGPD.

—*Protección de datos por defecto*. Solo serán objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. En particular, los datos personales no serán accesibles, por defecto, a un número indeterminado de personas físicas[57].

¿Cómo puede demostrar el responsable que ha aplicado estas medidas?

La adhesión a códigos de conducta o a un mecanismo de certificación debidamente aprobados podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento[58].

Estas medidas, son, por ejemplo...

Para garantizar un nivel de seguridad adecuado al riesgo pueden incluirse, por ejemplo, estas medidas:

—la seudonimización y el cifrado de datos personales;

—la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento

—la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico

—un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento[59].

[54] Art. 34.3 RGPD.
[55] Art. 33.2 RGPD.
[56] Art. 24.1 RGPD.
[57] Art. 25 RGPD.
[58] Art. 24.3 RGPD.
[59] Art. 32 RGPD.

¿Cómo se fijan los deberes y derechos del encargado del tratamiento?

El tratamiento por el encargado se regirá por un contrato que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

El contenido mínimo de este contrato se fija en el art. 28 del RGPD. La AEPD da algunas indicaciones para su redacción en el documento "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento" (`www.agpd.es`).

Además, si un encargado infringe la ley al determinar los fines y los medios del tratamiento, será considerado también responsable del tratamiento[60].

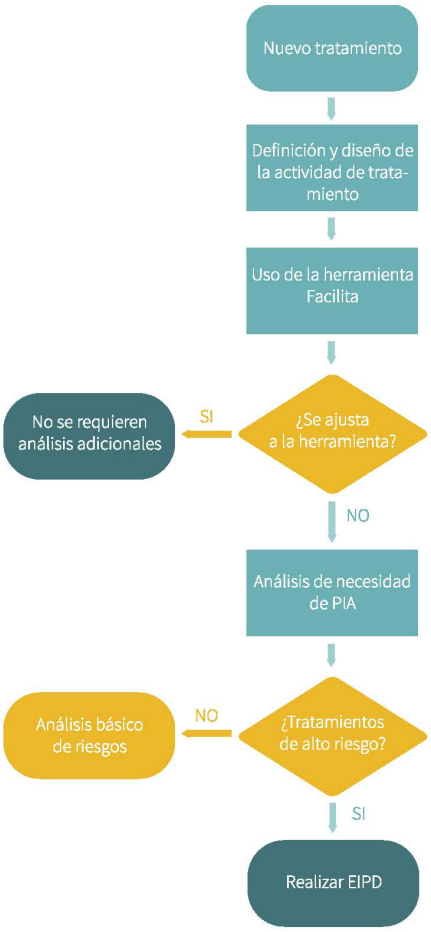

Figura 2: Categorías de análisis de riesgos (tomado de [2])

¿Cuándo es obligatorio realizar una* evaluación de impacto *previa al tratamiento?

[60] Art. 28.10 RGPD

Es necesario realizar una evaluación de impacto de protección de datos (EIPD) cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, entrañe un alto riesgo para los derechos y libertades de las personas físicas. En particular, es obligatorio en los siguientes casos:

—evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar

—tratamiento a gran escala de categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales

—observación sistemática a gran escala de una zona de acceso público[61] [62].

Análisis de riesgos, evaluación de impacto,. . . ¡Todo me parece lo mismo!

En realidad, no lo es. El análisis de riesgos ha de realizarse siempre. En casos sencillos, este análisis no es objeto de un documento especial; la herramienta "Facilita" de la AEPD (`www.agpd.es`) detecta estos casos sencillos. Cuando la herramienta "Facilita" no es aplicable, hay que realizar un análisis explícito de riesgos. Y solo en los casos previstos en la ley este análisis llevará a una evaluación de impacto. Esto se esquematiza en la figura 2, tomada de [2]. En el mismo documento [2] se proporcionan plantillas para la elaboración del análisis de riesgos. Y en el documento [3] se ejemplifica una metodología para la elaboración de la EIPD y se proporcionan catálogos de amenazas y soluciones y plantillas para las diversas fases de la EIPD.

¿En qué consiste la figura del* Delegado de protección de datos*?

Es una persona, designada atendiendo a sus cualidades profesionales, a sus conocimientos especializados del Derecho y a su práctica en materia de protección de datos[63], que es parte de la plantilla del responsable o del encargado, o desempeña sus funciones en el marco de un contrato de servicios[64].

Sus funciones, como mínimo, serán informar y asesorar al responsable y encargado y a sus empleados, supervisar el cumplimiento de lo dispuesto en la legislación, y cooperar y comunicarse con la autoridad de control (la AEPD)[65].

El delegado de protección de datos no recibirá ninguna instrucción del responsable o el encargado en lo que respecta al desempeño de sus funciones, ni será destituido ni sancionado por desempeñarlas[66].

¿Cuándo es necesario designar un Delegado de protección de datos?

Cuando

—el tratamiento lo lleve a cabo una autoridad u organismo público;

—las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala;

[61] Art. 35 RGPD.

[62] El RGPD prevé que la autoridad de control (la AEPD) establezca una lista de tipos de tratamientos que requieren evaluación de impacto, y una lista de tipos de tratamiento que no la requieran.

[63] Art. 37.5 RGPD.

[64] Art. 37.6 RGPD.

[65] Art. 39 RGPD.

[66] Art. 38.3 RGPD.

—las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales, o de datos relativos a condenas e infracciones penales[67].

Referencias

[1] AEPD. Guía para el cumplimiento del deber de informar. Informe t'ecnico, AEPD, 2018.

[2] AEPD. Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD. Informe t'ecnico, AEPD, 2018.

[3] AEPD. Guía práctica para las evaluaciones de impacto en la protección de los datos personales sujetas al RGPD. Informe t'ecnico, AEPD, 2018.

[67] Art. 37.1 RGPD.