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 febrero de 2020

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 directamente aplicable en España el *Reglamento General de Protección de Datos* (RGPD) publicado por la Unión Europea en mayo de 2016[3]. Esta norma europea se complementa con la *Ley Orgánica de Protección de Datos Personales* (LOPDGDD)[4].

¿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.

También existen agencias en algunas comunidades autónomas, con competencias en los tratamientos de datos de que sean responsables las entidades autonómicas y locales.

Además, para garantizar la aplicación coherente del RGPD en toda la Unión Europea, existe el "Comité Europeo de Protección de Datos".

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

No; como hemos dicho, existe un órgano europeo de coordinación que puede emitir dictámenes vinculantes.

Por otra parte, las resoluciones de la AEPD son recurribles ante los tribunales, concretamente, ante la Audiencia Nacional[5] y, en última instancia, ante el Tribunal Supremo.

¿Y no se puede recurrir ante un tribunal europeo?

[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 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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

No. Sin embargo, los Tribunales españoles puede suspender el procedimiento para plantear una *cuestión prejudicial* ante el Tribunal de Justicia de la Unión Europea cuando tengan dudas sobre la aplicación de una norma comunitaria (como el RGPD) en una determinada causa.

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

En el caso de infracciones leves, o si una multa constituyese una carga desproporcionada para una persona física, la AEPD puede limitarse a *apercibir* al infractor. Pero, en general, la sanción consistirá en una *multa* que, según el RGPD, puede 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[6].

También puede imponer una limitación temporal o definitiva del tratamiento de datos, e incluso prohibirlo; y ordenar la rectificación o supresión de datos personales[7].

Para cada infracción, ¿cómo se determina la cuantía de la multa?

El RGPD[8] y la LOPDGDD[9] establecen algunos criterios de graduación. Sin embargo, hay que reconocer que el margen de discrecionalidad es muy grande y que —al menos por ahora— es muy difícil prever, dada una infracción, cuál será la sanción que le corresponda.

¿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 LOPDGDD?

¡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 pena de prisión y multa:

—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.

[6] Art. 83 RGPD.
[7] Art. 58 RGPD.
[8] Art. 58.2 RGPD.
[9] Art. 76 LOPDGDD.

—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[10].

Además, expresamente se tipifica como delito la conducta consistente en difundir, revelar o ceder a terceros, sin autorización de la persona afectada, imágenes o grabaciones audiovisuales que se hubieran obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona[11].

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

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

2. Tratamiento de datos

¿Qué datos se consideran* personales*?

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[12].

Esta persona física se denomina *el interesado*.

¿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[13].

Entonces, ¿los datos seudonimizados son datos anónimos?

No. Los datos seudonimizados no son datos *anónimos*. Información anónima es la que no guarda relación con una persona física identificada *o identificable*. El RGPD no afecta al tratamiento de la información anónima, inclusive con fines estadísticos o de investigación, pero sí al tratamiento de los datos seudonimizados[14].

¿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[15].

[10] Arts. 197 y 198 del Código Penal.
[11] Arts. 197.7 del Código Penal.
[12] Art. 4 RGPD.
[13] Art. 4 RGPD.
[14] Considerando 26 RGPD.
[15] vd. sentencia de la Audiencia Nacional de 1 septiembre 2011.

¿Son las* imágenes *datos personales?

Sí, según criterio constante de la AEPD y de la Audiencia Nacional. La AEPD ha publicado un documento titulado *Protección de datos: Guía sobre el uso de videocámaras para seguridad y otras finalidades* (29 de Junio de 2018) y disponible en su sitio web[16] donde se dan instrucciones detalladas sobre la forma en que se deben tratar estos datos.

¿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 transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción[17].

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;

—genéticos y biométricos dirigidos a identificar de manera unívoca a una persona física;

—relativos a la salud;

—relativos a la vida sexual o la orientación sexuales de una persona física.

El tratamiento de estos datos está sometido a restricciones adicionales[18].

¿A qué tratamientos de datos se aplica el RGPD?

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[19].

¿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[20].

¿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

[16] `https://www.aepd.es/media/guias/guia-videovigilancia.pdf`
[17] Art. 4 RGPD.
[18] Art. 9 RGPD.
[19] Art. 2 RGPD.
[20] Art. 4 RGPD.

de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención[21].

¿Qué es una actividad exclusivamente personal o doméstica?

La que no tiene conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades[22]. Las Autoridades de control y los Tribunales tienden a interpretar esta *excepción doméstica* de forma muy restrictiva.

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

La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento[23].

¿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[24].

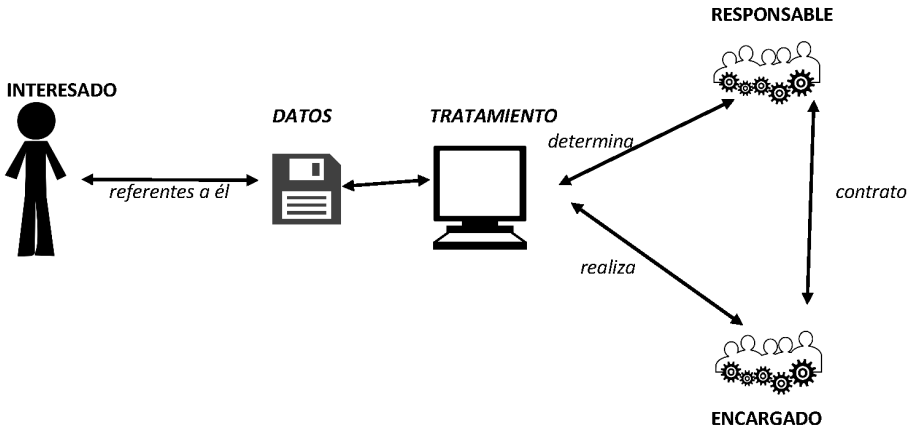

Figura 1: Roles jurídicos en el tratamiento de datos

Cuestión 1 La Universidad de Villalquite tiene como Rector a don Numerio Negidio. Dentro de la Universidad existe un Servicio de Informática, responsable entre otras cosas del procesamiento de los datos de matrícula de los alumnos. La Directora del Servicio es doña Lucía Ticia.

Indicar, caso de que existan, quiénes son (i) el o los interesados en el tratamiento de los datos de matrícula; (ii) el o los responsables del tratamiento; (iii) el o los encargados del tratamiento.

[21] Art. 2 RGPD.
[22] Considerando 18 RGPD.
[23] Art. 4 RGPD.
[24] Art. 4 RGPD.

Cuestión 2 Tras acabar sus estudios en la Universidad de Villalquite, don Estico Estíquez trabaja como asesor fiscal autónomo. Uno de sus clientes es la empresa "*Kkfashion, Escuela de modelos*", que le tiene encomendada la gestión de su contabilidad (facturas, clientes, proveedores, alumnos, ...)

Indicar, caso de que existan, quiénes son (i) el o los interesados en el tratamiento de los datos de contabilidad; (ii) el o los responsables del tratamiento; (iii) el o los encargados del tratamiento.

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[25].

¿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[26].

¿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[27].

¿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[28].

¿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[29].

Todas las personas que intervengan en cualquier fase del tratamiento estarán sujetas al deber de confidencialidad[30].

[25] Art. 5.1 RGPD.
[26] Art. 5.1 RGPD.
[27] Art. 5.1 RGPD.
[28] Art. 5 RGPD.
[29] Art. 5.1 RGPD.
[30] Art 5 LOPDGDD.

¿En qué consiste el principio de* responsabilidad proactiva[31] *?

El responsable del tratamiento será responsable del cumplimiento de todos los principios anteriores y debe ser capaz de demostrarlo[32].

¿En qué consiste el* principio de legitimación *del tratamiento?

El tratamiento solo será lícito si se da al menos una de las *causas o bases de legitimación* enunciadas en el RGPD[33].

¿Cuáles son las bases de legitimación enunciadas en el RGPD?

La primera de ellas es el *consentimiento del interesado* para el tratamiento de sus datos para uno o varios fines específicos.

¿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[34].

El responsable deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales[35].

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[36].

¿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?

[31] En inglés, "accountability". Una traducción quizás mejor sería "rendición de cuentas".
[32] Art. 5.2 RGPD.
[33] Art. 6.1 RGPD.
[34] Art. 4.11 RGPD
[35] Art. 7.1 RGPD
[36] Art. 7.2 y 4 RGPD

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[37].

La ley española establece que el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico[38].

¿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[39].

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

El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela[40].

¿Cuáles son las restantes bases de legitimación?

El RGPD establece otras cinco bases:

—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[41].

Eso del "interés legítimo", ¿en qué consiste?

Es difícil de concretar, ya que en principio cualquier finalidad que no vaya contra la ley puede fundamentar un interés legítimo. El RGPD da algunos ejemplos[42] y por su parte la LOPDGDD[43] establece que en algunos casos se presume el interés legítimo.

[37] Art. 9 RGPD
[38] Art. 9 LOPDGDD.
[39] Art. 7.3 RGPD.
[40] Art. 7 LOPDGDD.
[41] Art. 6.1 RGPD.
[42] Considerando 47 RGPD.
[43] Arts. 19 a 23 LOPDGDD.

¿Cuáles son esos casos en que se presume el interés legítimo?

Entre otros:

—El tratamiento de los datos de contacto y relativos a la función o puesto desempeñado por las personas físicas que presten servicios en una persona jurídica siempre que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional y la finalidad del tratamiento sea únicamente mantener relaciones con dicha persona jurídica

—El tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

—el tratamiento de datos que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

Y también los llamados coloquialmente "ficheros de morosos" (siempre que se cumplan ciertos requisitos):

—el tratamiento de datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia.

¿Pueden los particulares instalar sistemas de videovigilancia, basándose en su interés legítimo??

Sí, siempre que respeten los principios generales del tratamiento de datos. Ello supone, entre otras cosas, lo siguiente:

—Una persona física puede tratar imágenes que solamente capten el interior de su propio domicilio.

—Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad de preservar la seguridad de personas y bienes[44].

—Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones[45].

—Es necesario valorar si realmente es necesaria la instalación de la videovigilancia o si el fin perseguido se puede alcanzar de otra forma. También es necesario tener en cuenta la proporcionalidad en función del número de cámaras, tipo de las mismas y la opción de utilizar "máscaras de privacidad".

—El deber de información exige colocar en las zonas videovigiladas un dispositivo informativo ubicado en lugar suficientemente visible[46].

4. Derechos del interesado

¿Qué derechos tiene el interesado frente al responsable del tratamiento?

Tradicionalmente se han llamado "derechos ARCO", por las siglas de acceso, rectificación, cancelación (ahora llamado supresión) y oposición. El RGPD añade los derechos de limitación y de portabilidad. La LOPDGDD concreta además el

[44] Art. 22.1 y 22.2 LOPDGDD.
[45] Art. 22.3 LOPDGDD.
[46] Art. 22.3 LOPDGDD.

llamado "derecho al olvido" frente a servicios de indexación y recuperación de la información.

¿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[47]. Si es así, tiene derecho a acceder a tales datos personales y a ser informado sobre el origen de los mismos y el uso que se les da.

El responsable facilitará una copia de los datos personales objeto de tratamiento[48].

¿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[49].

¿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:

—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[50].

¿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[51].

¿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[52].

[47] Art. 15.1 RGPD.
[48] Art. 15.3 RGPD.
[49] Art. 16.1 RGPD.
[50] Art. 17.1 RGPD.
[51] Art. 21 RGPD.
[52] Art. 4 RGPD.

¿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[53].

¿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[54].

¿Cómo puede el interesado ejercer estos derechos?

El procedimiento no requiere de ninguna formalidad específica y no supone ningún coste económico para el interesado. El interesado se dirigirá al resposable por cualquier medio idóneo (la AEPD proporciona modelos para el ejercicio de estos derechos[55].) Si el responsable no atiende la petición del interesado, este puede presentar una reclamación ante la Autoridad de control (por ejemplo, telemáticamente). También puede acudir a los Tribunales (esto último en general sí supondrá un coste económico para el interesado).

¿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[56].

¿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.

[53] Art. 22 RGPD.
[54] Art. 18 RGPD.
[55] `https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos`
[56] Art. 20 RGPD.

¿Reconoce la ley el derecho al olvido?

Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información. Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet. Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo[57].

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;

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[58].

¿Cómo hay que facilitar toda esa información?

[57] Art. 93 LOPDGDD.
[58] Art. 13 RGPD.

Puede indicarle una dirección electrónica u otro medio que permita acceder a ella de forma sencilla e inmediata. Pero siempre debe proporcionarle directamente la siguiente información básica:

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

b) los fines del tratamiento a que se destinan los datos personales;

c) la posibilidad de ejercer sus derechos[59].

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia.

En la figura 2 aparece un ejemplo de presentación de esta información básica o de primer nivel, que obligatoriamente debe mostrarse. El ejemplo está tomado de la "Guía para el cumplimiento del deber de informar" publicada por la AEPD en 2018[60] .

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 2: Información al interesado (nivel básico)

¿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[61].

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

Sí. El responsable no está obligado a facilitar ninguna información

—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[62].

[59] Art. 11 LOPDGDD.

[60] `https://www.aepd.es/sites/default/files/2019-11/guia-modelo-clausula-informativa.pdf`

[61] Art. 14.1 y 2 RGPD.

[62] Art. 14.4 RGPD.

¿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[63].

¿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[64], 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[65].

¿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[66].

También la documentará, incluyendo los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas[67].

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[68]. No obstante, si los datos estaban cifrados, no es necesaria la comunicación al interesado, ni 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[69].

[63] Art. 30 RGPD.
[64] `https://www.aepd.es/es/la-agencia/transparencia/otro-tipo-de-informacion/registro-actividades-tratamiento-aepd`
[65] Art. 4 RGPD.
[66] Art. 33.1 RGPD.
[67] Art. 33.5 RGPD.
[68] Art. 34.1 RGPD.
[69] Art. 34.3 RGPD.

¿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[70]. La AEPD ha elaborado una "Guía para la gestión y notificación de las brechas de seguridad"[71].

¿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"[72].

Además, si un encargado infringe la ley al determinar los fines y los medios del tratamiento, será considerado también responsable del tratamiento[73].

¿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[74], que es parte de la plantilla del responsable o del encargado, o desempeña sus funciones en el marco de un contrato de servicios[75].

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)[76].

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[77].

¿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;

—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[78].

¿Podemos concretar algo más?

[70] Art. 33.2 RGPD.
[71] `https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf`
[72] `https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf`
[73] Art. 28.10 RGPD
[74] Art. 37.5 RGPD.
[75] Art. 37.6 RGPD.
[76] Art. 39 RGPD.
[77] Art. 38.3 RGPD.
[78] Art. 37.1 RGPD.

En la LOPDGDD figura una lista no exhaustiva de entidades que obligatoriamente deben designar un Delegado de protección de datos[79]. Por ejemplo:

a) Los colegios profesionales.

b) Los centros docentes de cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad. .

6. Seguridad, análisis de riesgos y evaluación de impacto

¿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[80]

En particular, deberá aplicar los principios de *Protección de datos desde el diseño* del sistema de información y *Protección de datos por defecto*.

¿En qué consiste la* protección de datos desde el diseño*?

Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, *tanto en el momento de determinar los medios de tratamiento* como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas para aplicar de

[79] Art. 34 LOPDGDD.
[80] Art. 24.1 RGPD.

forma efectiva los principios de protección de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados[81].

La AEPD ha publicado una "Guía de privacidad desde el diseño"[82].

¿En qué consiste la* 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[83].

¿Cómo puede demostrar el responsable que ha aplicado las medidas apropiadas?

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[84].

¿Qué medidas son concretamente las que hay que adoptar?

El RGPD no las concreta. Sí dice que, tras el correspondiente análisis, para garantizar un nivel de seguridad adecuado al riesgo pueden incluirse medidas que incluyan:

—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[85].

Entonces, ¿qué hay que hacer para determinar las medidas concretas que se deben adoptar?

Como se ha dicho, ya, las medidas son el resultado de un *análisis de riesgos*. En los tratamientos de bajo riesgo, este análisis no es objeto de un documento especial; la herramienta "Facilita" de la AEPD[86] detecta estos casos de bajo riesgo y recomienda para ellos un conjunto de medidas. Además, "Facilita" genera la documentación necesaria para cumplir otros deberes (información, registro de actividades, etc.).

¿Y si el tratamiento no es detectado como de bajo riesgo y "Facilita" no es aplicable?

Cuando la herramienta "Facilita" no es aplicable, hay que realizar un análisis explícito de riesgos. Y en los casos previstos en la ley este análisis llevará a una

[81] Art. 25.1 RGPD.
[82] `https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf`
[83] Art. 25.2 RGPD.
[84] Art. 24.3, 25.3 y 32.3 RGPD.
[85] Art. 32.1 RGPD.
[86] `https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd`

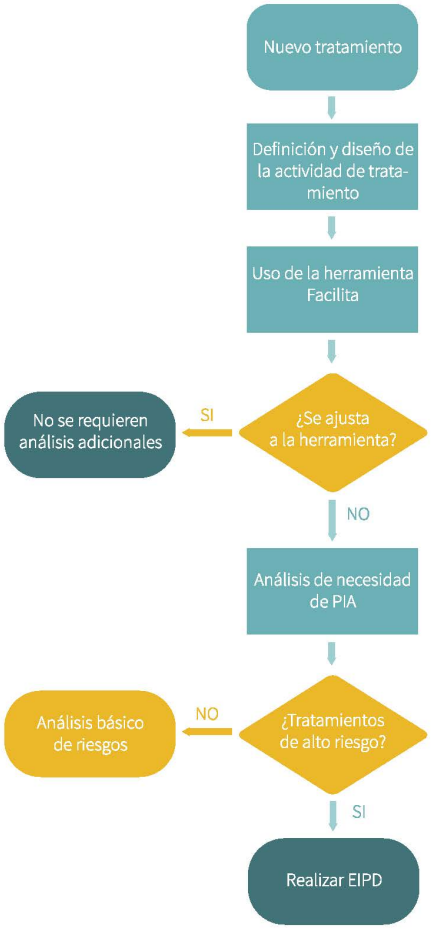

Figura 3: Categorías de análisis de riesgos (tomado de la *Guía de Análisis)*

evaluación de impacto. Esto se esquematiza en la figura 3, tomada de la "Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD"[87].

En el mismo documento se proporcionan plantillas para la elaboración del análisis de riesgos. Y en el documento "Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD"[88] 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.

La AEPD ofrece libre y gratuitamente una herramienta "Gestiona EIPD" para la realización tanto de análisis simple de riegos como de EIPD[89].

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

[87] `https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf`
[88] `https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf`
[89] `https://gestiona.aepd.es/`

tratamiento?

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[90].

¿Podemos concretar algo más los casos en los que hay "un alto riesgo"?

El RGPD prevé que la autoridad de control (la AEPD) establezca una lista de tipos de tratamientos que requieren evaluación de impacto. La AEPD ha publicado recientemente esta lista[91]. Por ejemplo, debe realizarse un EIDP en los siguientes casos:

—Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.

—Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.

—Tratamientos que impliquen el uso de datos genéticos para cualquier fin.

—Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.

—Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.

—Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato.

[90] Art. 35 RGPD.

[91] `https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf`