Derechos del afectado

PID_00246874

Antoni Roig

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Antoni Roig

Índice

1. Derechos tradicionales

No todos los derechos reconocidos en el RGPD son nuevos. Algunos de ellos ya existían en la Directiva 95/46/CE, como el derecho a ser informado del tratamiento de los datos personales y los derechos ARCO, es decir, de acceso, rectificación, cancelación y oposición. Empezaremos, pues, por estos derechos para pasar, a continuación, a los nuevos derechos incorporados por el Reglamento 2016/679.

1.1. Transparencia de la información y comunicación: el derecho a ser informado

El artículo 12 RGPD obliga al responsable del tratamiento de los datos a facilitar al interesado toda la información referida en los artículos 13 y 14[1] (Hernández, 2016). La información[2] deberá constar «en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño» (art. 12 RGPD y art. 21 APLOPD). La información puede adoptar diferentes formatos, ya sea por escrito o por medios electrónicos. Si el interesado lo solicita, se podrá facilitar verbalmente, siempre que se demuestre la identidad del interesado por otros medios. La información facilitada será a título gratuito. Una novedad del Reglamento 2016/679 consiste en la posibilidad de facilitar la información en combinación con iconos normalizados que faciliten la comprensión del interesado (art. 12,7 RGPD). Con esta finalidad, la Comisión especificará la información que se podrá presentar mediante iconos y los procedimientos para proporcionar iconos normalizados.

(1)El art. 5a) RGPD incorpora, además de la licitud y lealtad del tratamiento, ya presentes en el art. 6a) de la Directiva 95/46/CE, la transparencia. Este principio resulta especialmente importante en el contexto actual de proliferación de agentes y de complejidad tecnológica (considerando 58 del RGPD).

(2)Agencia Española de Protección de Datos, Autoridad Catalana de Protección de Datos, Agencia Vasca de Protección de Datos (2016), *Guía para el cumplimiento del deber de informar*.

Lectura recomendada

J. A. Hernández (2016). «Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 205-226). Madrid: Ed. Reus.

Se distinguen dos supuestos: cuando los datos se obtengan del interesado (art. 13 RGPD) y cuando los mismos no se hayan obtenido del interesado (art. 14 RGPD).

1) Información que hay que facilitar cuando los datos personales se obtengan del interesado (art. 13.1 RGPD)

- Identidad y datos de contacto del responsable.
- Datos de contacto del delegado, si lo hubiera.

- Finalidad y justificación legal del tratamiento de los datos.

- Cuando se alegue que «el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento» (art. 6.1f RGPD), estos deberán especificarse.

- Destinatarios o categorías de destinatarios, en su caso.

- Intención, en su caso, de transferir los datos a un tercer país u organización internacional y referencia a las garantías adecuadas.

En el momento en que se obtengan los datos personales, se deberá, además, informar sobre los siguientes aspectos:

- El plazo durante el cual se conservarán los datos personales, o si no es posible determinarlo, los criterios para determinar este plazo.

- Derecho a solicitar al responsable el acceso, rectificación y supresión de los datos, o la limitación u oposición a su tratamiento, y derecho a la portabilidad de los datos.

- Derecho a retirar el consentimiento previo prestado.

- Derecho a presentar una reclamación ante una autoridad de control.

- La existencia de decisiones automatizadas, incluyendo la elaboración de perfiles, con información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2) Información suplementaria que hay que facilitar cuando los datos personales no se hayan obtenido del interesado (art. 14.1 RGPD)

- Categorías de datos de la que se trate.
- La fuente de la que proceden los datos y, en su caso, si proceden de fuentes de acceso público.

La información se facilitará, sin necesidad de requerimiento alguno, en un plazo razonable:

- antes de un mes, una vez obtenidos los datos personales,
- antes o en el momento de la primera comunicación al interesado,
- antes de comunicar los datos a otro destinatario.

El responsable deberá poder acreditar con posterioridad que, efectivamente, ha cumplido con su obligación de informar. Si el responsable piensa tratar más adelante los datos para otra finalidad distinta de la que fueron inicialmente

recopilados, tendrá que informar, antes de iniciar el tratamiento con distinta finalidad, sobre el nuevo fin. No será necesario informar si el interesado ya dispone de la información. En el supuesto de que la información no proceda del interesado, la novedad es que la información no se enviará si resulta imposible, supone un esfuerzo desproporcionado o dificulta los objetivos del tratamiento de los datos. Una alternativa a la comunicación podrá ser, entonces, hacer pública la información. Tampoco se informará al interesado cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional.

Tabla 1. Resumen de la *Guía para el cumplimiento del deber de informar* (AEPD, 2016)

Epígrafe	**información básica (1.ª capa, resumida)**	**información adicional (2.ª capa, detallada)**
«Responsable» (del tratamiento)	Identidad del responsable del tratamiento	Datos de contacto del responsable
		Identidad y datos de contacto del representante
		Datos de contacto del delegado de protección de datos
«Finalidad» (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
«Legitimación» (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo
		Obligación o no de facilitar datos y consecuencias de no hacerlo
«Destinatarios» (de cesiones o transferencias)	Previsión o no de cesiones	Destinatarios o categorías de destinatarios
	Previsión de transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
«Derechos» (de las personas interesadas)	Referencia al ejercicio de derechos	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la autoridad de control
«Procedencia» (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se tratan

El epígrafe «Procedencia» se añadirá cuando los datos no procedan del propio interesado. En cuanto al ejercicio del derecho, algunas de las formas para informar pueden ser las mismas que para la recogida de los datos: formularios en papel, formularios web, entrevista telefónica o aplicaciones móviles, entre otras. Si las comunicaciones sobre datos están ya disponibles, o se requieren tratamientos adicionales, pueden hacerse por medio de correo postal, mensajería electrónica o notificaciones emergentes en servicios y aplicaciones. La información básica se presentará preferentemente en forma de tabla, con una visibilidad equivalente a una información nutricional alimentaria. El apartado «Legitimación» se refiere a:

- Ejecución de un contrato.
- Cumplimiento de una obligación legal.
- Misión en interés público o ejercicio de poderes públicos.
- Interés legítimo del responsable.
- Interés legítimo de un tercero.
- Consentimiento del interesado.

La AEPD ofrece un ejemplo ilustrativo de sus recomendaciones para la información básica:

Tabla 2. Ejemplo de información básica

Información básica sobre protección de datos	
Responsable	Ediciones X, S. A.
Finalidad	Gestión de la suscripción.
Legitimación	Ejecución de un contrato.
Destinatarios	No se cederán datos a terceros, salvo obligación legal.
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Podéis consultar la información adicional y detallada sobre protección de datos en nuestra página web.

Fuente: AEPD (2016).

La información adicional se refiere a la segunda capa detallada en el cuadro anterior. En cuanto a la información adicional sobre el responsable, consistirá en la identidad y CIF, la dirección postal, el teléfono, correo electrónico y los datos de contacto del delegado de protección de datos, es decir, una web o correo electrónico. La información adicional sobre la finalidad puede consistir, por ejemplo, en «facilitar a los interesados ofertas de productos y servicios de su interés» o «para mejorar su experiencia como usuario, elaboraremos un perfil comercial según la información. No se tomarán decisiones automatizadas a partir de dicho perfil». También se añadirá una referencia al tiempo de conservación, como por ejemplo, «mientras se mantenga la relación comercial». En cuanto a la legitimación para el tratamiento, puede consistir en «la ejecución del contrato de suscripción a la revista X». Los destinatarios de los

datos serán, por ejemplo, «otras firmas del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados». Finalmente, en cuanto a la procedencia, se podrá mencionar, por ejemplo, que «proceden de otras empresas de nuestro grupo» y las categorías de datos son datos de identificación, direcciones postales o electrónicas, información comercial y datos económicos, pero no se tratan datos especialmente protegidos.

Como en todos los derechos, hay excepciones. Así, algunas circunstancias pueden hacer que el deber de información no sea necesario, pues ya se dispone de la información (arts. 13.4 y 14.5 RGPD); en otros casos, el deber de informar cede frente a bienes jurídicos prevalentes (art. 23 RGPD).

1.2. Derechos ARCO: acceso, rectificación, cancelación y oposición

1) Derecho de acceso

La centralidad del derecho de acceso proviene de su aspecto instrumental respecto al ejercicio de los demás derechos: únicamente sabiendo los datos que obran en poder del responsable, puede entonces valorarse si se cumplen las exigencias del RGPD y ejercer los derechos contemplados en los arts. 16-22 RGPD. El interesado tiene derecho a que el responsable le confirme si está tratando datos personales que le conciernen y, entonces, acceder a la siguiente información (art. 15 RGPD y art. 23 APLOPD)[3]:

(3)Los contenidos son los mismos que en el art. 12 de la Directiva 95/46/CE y el art. 15 LOPD. Faltan únicamente la base jurídica del tratamiento y el interés legítimo, aunque cabe entender que también se encuentran incluidos en el derecho de acceso.

- Fines del tratamiento.
- Categorías de datos.
- Destinatarios o categorías de destinatarios[4].

(4)La información relativa al tratamiento, como son los destinatarios y, por tanto, no solo los datos personales del interesado en sentido estricto, queda cubierta por el derecho de acceso. Esto se menciona en el art. 154 RGPD, al indicar el derecho de acceso «a los datos personales y a la siguiente información». Quizá el amplio entendimiento del grupo de trabajo del art. 29 y el del TJUE sobre el concepto de «datos personales» también habrían permitido llegar a la misma conclusión si el art. 15 RGPD se hubiera limitado a mencionar simplemente los datos personales (Hernández, 2016, págs. 223-224). Opinión 4/2007. *On the concept of personal data* (pág. 10); STJUE C-553/07, caso Rotterdam contra Rijkeboer, párrafos 42 y 43.

- Si es posible, el plazo de conservación o, en todo caso, los criterios para determinarlo.
- El derecho a solicitar la rectificación o supresión de los datos, así como la limitación u oposición al tratamiento.
- El derecho a presentar una reclamación ante una autoridad de control.
- Cuando los datos no se han obtenido del interesado, cualquier información disponible sobre el origen.
- La existencia de decisiones automatizadas, incluyendo la elaboración de perfiles, con información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
- Las garantías de la transferencia a un tercer país u organización internacional, si se da el caso.

Lectura recomendada

Sobre la centralidad del derecho de acceso en el marco general de la protección de datos, podéis leer el siguiente trabajo:

A. Troncoso (2010). *La protección de datos personales. En busca del equilibrio* (pág. 111 y siguientes). Valencia: Tirant lo Blanch.

El responsable facilitará una copia de los datos personales, siempre que no afecte a derechos de tercero. El responsable podrá percibir un canon razonable por las copias adicionales. Si el interesado presenta la solicitud por medios electrónicos, la información se facilitará en un formato electrónico de uso común. En este sentido, en el art. 23 APLOPD se dice que se entenderá otorgado el derecho de acceso si el responsable facilita un acceso remoto, directo y seguro a los datos personales. Como regla general, se considerará repetitivo el ejercicio del derecho en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello (art. 23.4 APLOPD).

En la Directiva 95/46/CE, debían facilitarse los datos, pero no así las copias, con la excepción de la historia médica. En el RGPD, en cambio, se reconoce el derecho a obtener una copia de los datos personales tratados. En todo caso, no hay derecho a obtener un certificado (Hernández, 2016, pág. 224).

2) Derecho de rectificación, supresión o cancelación, y derecho de oposición

Los llamados derechos ARCO (acceso, rectificación, cancelación y oposición), con el RGPD, pasan a ser derechos de transparencia, información, acceso, rectificación, y supresión o derecho al olvido, limitación del tratamiento, portabilidad y oposición (Piñar). El interesado tiene derecho a obtener del responsable, sin dilación indebida, la rectificación de los datos inexactos que le conciernan (art. 16 RGPD). En este sentido, y de acuerdo con los fines del tratamiento, podrá solicitar que le completen los datos faltantes, e incluso añadir alguna declaración adicional. Para ello, deberá indicarse a qué datos se refiere y qué corrección hay que hacer (art. 24 APLOPD). En este mismo artículo se contempla la posibilidad, en ocasiones, de acompañar la solicitud con documentación que justifique la corrección que hay que hacer. Los estados miembros podrán establecer especificaciones y excepciones cuando se trate de datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos[5].

(5)Considerando 156 del RGPD. También, de manera más general, se mencionan restricciones a los derechos en el considerando 73 del RGPD.

Lecturas recomendadas

Sobre el derecho del interesado a la rectificación de los datos, véase:

M. Álvarez (2016b). «El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 227-256). Madrid: Ed. Reus.

Considerando 65 del RGPD. El derecho de rectificación carece en la Directiva 95/46/CE de un artículo propio, y se encuentra dentro del art. 12, llamado «derecho de acceso».

De igual manera, el interesado tiene derecho a que se supriman o cancelen los datos personales que le conciernen en los siguientes casos (art. 17 RGPD)[6] (Álvarez, 2016b, pág. 234):

(6)El RGPD ha cambiado el tradicionalmente llamado «derecho a la cancelación de los datos» por la nueva denominación de «derecho a la supresión». El contexto es más amplio, pues incluye la supresión en el caso de los motores de búsqueda u otros responsables del tratamiento en Internet, es decir, el derecho al olvido, que veremos en otro apartado.

- Cuando ya no sean necesarios para la finalidad con la que fueron recopilados.
- Cuando el interesado se oponga, salvo que el responsable acredite motivos legítimos suficientes, como veremos.
- Cuando los datos han sido tratados ilícitamente.
- Cuando se cumpla una obligación legal.
- Cuando se trate de ofertas directas a niños de servicios de la sociedad de la información.

De acuerdo con el art. 25.2 APLOPD, cuando la supresión derive del derecho de oposición, el responsable podrá conservar los datos de identificación del afectado para impedir futuros tratamientos de mercadotecnia directa. Para suprimir los datos personales, el responsable adoptará las medidas razonables necesarias, teniendo en cuenta la tecnología disponible y el coste de su apli-

cación. Existen, sin embargo, algunas excepciones a la obligación de suprimir los datos (art. 17.3 RGPD). En efecto, en ocasiones el tratamiento de los datos es necesario:

- En ejercicio del derecho a la libertad de expresión e información.
- Para cumplir una obligación legal europea o nacional.
- Por razones de interés público en el ámbito de la salud pública.
- Con fines de archivo en interés público, investigación científica o histórica, o fines estadísticos.
- Para formular o defenderse de reclamaciones.

El responsable informará de cualquier rectificación, supresión de datos personales o limitación del tratamiento, que veremos más adelante, a los destinatarios, a menos que ello sea imposible o suponga un esfuerzo desproporcionado. Si el interesado lo solicita, el responsable le informará sobre los destinatarios.

Finalmente, el interesado tiene derecho a oponerse al tratamiento de datos, siempre que no sean necesarios para cumplir una misión llevada a cabo en interés público o para satisfacer intereses legítimos (art. 21 RGPD). Por tanto, a menos que se acrediten motivos legítimos imperiosos, se dejarán de tratar los datos en cuestión[7]. Concretamente, podrá oponerse en cualquier momento cuando los datos tengan por finalidad la mercadotecnia directa, y los perfiles relacionados con la misma (considerando 70 del RGPD). El responsable informará de manera clara al interesado de este derecho de oposición en la primera comunicación con el mismo. El ejercicio de este derecho de oposición podrá hacerse por medios automatizados. Si los datos se tratan con fines de investigación científica, histórica o estadística, será posible, a pesar de ello, oponerse a su tratamiento, salvo que sea necesario para cumplir una misión de interés público. El art. 29 APLOPD contempla una obligación de bloqueo de los datos en los casos previstos en los arts. 16 y 17.1a, d, y e RGPD y cuando deba proceder de oficio a su rectificación o supresión. Los datos quedarán disponibles para los tribunales, el Ministerio Fiscal y otras administraciones públicas, como la AEPD, para la exigencia de posibles responsabilidades, hasta su prescripción. LA AEPD y las autoridades autonómicas podrán fijar excepciones a esta obligación de bloqueo.

[7]De acuerdo con el considerando 69, el interesado puede oponerse al tratamiento de datos relativos a su situación personal, y entonces el responsable tendrá la carga de probar los intereses legítimos imperiosos que prevalecen sobre los intereses o derechos del interesado.

2. Nuevos derechos

El RGPD incorpora, al menos, dos novedades importantes que guiarán la interpretación de los derechos previstos en el RGPD. La primera es el principio de responsabilidad proactiva o *accountability*, que tendremos ocasión de ver más adelante; el segundo es el enfoque de riesgo para los derechos, que hará que algunas garantías complementarias sean necesarias en el supuesto de nivel de riesgo alto y tipo de riesgo que plantea más problemas[8]. Pues bien, en este contexto, veamos ahora los nuevos derechos incluidos en el RGPD. Empezaremos por el derecho al olvido, veremos a continuación el derecho a la portabilidad, el derecho a no ser objeto de decisiones individuales automatizadas y, finalmente, el derecho a la limitación del tratamiento. Acabaremos este apartado con las limitaciones generales a los derechos previstos en el RGPD.

[8]Agencia Española de Protección de Datos, Autoridad Catalana de Protección de Datos, Agencia Vasca de Protección de Datos (2016). *Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento*.

2.1. Derecho al olvido

Ya hemos tenido ocasión de describir el derecho a la supresión de los datos. Pues bien, una novedad vinculada al mismo, y por tanto no considerada como un auténtico derecho autónomo, es el «derecho al olvido». Se trata, así, de una consecuencia de la aplicación del derecho a la supresión de datos, en un entorno muy concreto como es Internet. Este derecho consiste en la posibilidad de solicitar al responsable que suprima también cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos (art. 17 RGPD)[9]. Por tanto, es una manifestación del derecho de cancelación u oposición, siguiendo la jurisprudencia del Tribunal de Justicia de la UE en el caso Google Spain[10]. En este sentido, los motores de búsqueda son responsables de tratamiento de datos. Y no solo ellos, cualquier responsable del tratamiento, como un prestador de servicios de la sociedad, una red social, blogs, o una plataforma de comercio electrónico. El contenido del derecho consiste en poder reclamar la supresión de los enlaces a páginas webs de terceros que contengan información sobre el interesado entre la lista de resultados obtenidos al llevar a cabo una búsqueda basada en un nombre de una persona[11] (Álvarez, 2016a, págs. 242-243).

[9]Sobre los motivos de incorporar esta vertiente tecnológica al derecho de supresión, véanse los considerandos 6 y 7 del RGPD. También está relacionado con el principio de calidad del dato (art. 5.1d RGPD), de finalidad (art. 5.1b RGPD), de proporcionalidad (art. 5.1c RGPD), minimización de los datos (art. 5.1c RGPD) y consentimiento (art. 6 RGPD) y licitud (art. 7 RGPD).

[10]Caso C-131/12, *Google Spain SL and Google Inc. c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González ('Google Spain')*, de 13 de mayo del 2014. El grupo de trabajo del artículo 29 tiene una guía sobre cómo desarrollar los elementos de esta sentencia (WP225).

[11]El derecho no se limita a motores de búsqueda, sino a todos los responsables del tratamiento en Internet.

Lecturas recomendadas

Con respecto al derecho al olvido, podéis leer los siguientes trabajos:

M. Álvarez (2016a). «El derecho a la supresión o al olvido». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 241-256). Madrid: Ed. Reus. En su apartado 4, podemos encontrar una descripción de la tramitación de la propuesta del art. 17 del RGPD.

R. Pazos (2015). «El mal llamado derecho al olvido en la era de Internet». *Boletín del Ministerio de Justicia* (núm. 2183, noviembre, año LXIX, pág. 40).

M. López (2014). «Derecho a la información y derecho al olvido en Internet». *La Ley Unión Europea* (núm. 17, julio, pág. 49).

M. Peguera (2015). «In the Aftermath of Google Spain: How the 'Right to Be Forgotten' is Being Shaped in Spain by Courts and the Data Protection Authority». *International Journal of Law and Information Technology* (vol. 23, núm. 4, págs. 325-347). doi: 10.1093/ijlit/eav016.

M. Peguera (2016). «The Shaky Ground of the Right to Be Delisted». *Vanderbilt Journal of Entertainment & Technology Law* (vol. 18, núm. 3, págs. 507-561).

Ahora bien, el ejercicio de este derecho no significa que se borre la información de la fuente original; esta seguirá siendo accesible mediante otras palabras de búsqueda o mediante acceso directo a la página web. En este sentido, el marco legal de los responsables de la publicación de la página web y del motor de búsqueda es distinto. Aunque la publicación del contenido en la página web sea legal, la difusión global, unida a su relación con otros datos de una persona, puede tener efectos desproporcionados sobre su privacidad, que lleven a considerarla contraria a la ley. Por eso, se garantiza el derecho al olvido. Esto no significa, sin embargo, que los buscadores deban controlar permanentemente toda la información alojada en sus servidores; deben, simplemente, responder a las solicitudes de los interesados que ejerzan su derecho al olvido. El interés general al acceso a la información que se quiere borrar debe ser tenido en cuenta a la hora de resolver la solicitud. Con todo, conviene recordar lo que hemos dicho anteriormente: el contenido borrado de la lista de resultados no se elimina por ello de la fuente original, y puede accederse todavía al mismo mediante búsqueda por otras palabras clave o accediendo directamente a la dirección de la página web.

Por otro lado, el interesado no debe contactar con la página web original para ejercer este derecho frente a los motores de búsqueda. Esto no es necesario, aunque puede hacerse si se cree conveniente. También puede solicitarse el borrado en más de un motor de búsqueda, con lo cual el interesado puede ampliar o reducir el impacto deseado. El procedimiento previsto al efecto por el responsable no es el único que puede seguir el interesado. Eso sí, el responsable debe comprobar en todo caso la identidad del solicitante. Para poder valorar la solicitud con fundamento, el interesado debe justificar adecuadamente la razón por la cual quiere borrar un resultado de la lista, indicando concretamente la URL que se quiere desvincular y si el interesado tiene un cargo público o no.

Otro aspecto importante y que no se da siempre en la práctica es que sacar de la lista de resultados una página debe tener efectos globales en todos los dominios, incluidos los .com. Por consiguiente, no se debería limitar la desvinculación a los dominios de los estados miembros o bien al .eu. Por otro lado, los responsables no tienen ninguna obligación de comunicar la desvinculación a los administradores de las páginas web desvinculadas. Si, para poder tener una mejor comprensión del contexto de la respuesta que hay que dar al interesado, el responsable contacta con el alojador de la página web en cuestión, entonces debe actuar de manera que preserve los derechos del interesado. Por consiguiente, la práctica de informar a los usuarios de los motores de búsqueda de que los resultados son incompletos, debido a la aplicación de la normativa europea de protección de datos, puede conducir a pensar que la petición de un usuario ha excluido resultados sobre otro usuario, lo que no es así. El motor de

búsqueda tampoco debe informar al administrador de la página web de que no se puede acceder a algunas páginas como resultado de una reclamación de un sujeto concreto indicado.

Cuando el responsable del motor de búsqueda deniega la solicitud, debe justificar suficientemente tal decisión[12]. Además, debe informar al interesado de que puede acudir a una autoridad de protección de datos si lo cree conveniente. En general, el derecho al olvido no puede ejercerse frente a motores de búsqueda internos o de efecto limitado. Por ejemplo, no sería de aplicación este derecho frente a los motores de búsqueda internos de las páginas webs de periódicos. Una buena práctica consistiría en publicar los criterios para resolver las solicitudes de desvinculación y ofrecer estadísticas de las resoluciones tomadas hasta el momento. Otra limitación consiste en la identidad del interesado, en principio, un ciudadano o residente en algún país miembro de la Unión Europea. En todo caso, una denegación podrá ser revisada por la autoridad de control o un tribunal competente, para que valore los criterios seguidos por la decisión del responsable. En este sentido, se tendrá en cuenta la presencia o no de los siguientes criterios para la decisión (WP 225):

(12)Esta posición parece situar el ejercicio del derecho al olvido en Internet sobre el derecho de oposición frente a motores de búsqueda. Sin embargo, hay autores que, a partir del artículo 17 RGPD, lo focalizan sobre las obligaciones del responsable principal de la web que ha hecho públicos los datos. Este es el caso, por ejemplo, de Troncoso (2013, pág. 33). La jurisprudencia del TJUE servirá para ir acotando los supuestos de aplicación del derecho al olvido, más allá del inicial caso Google Spain.

- ¿La búsqueda se refiere a una persona física? ¿El resultado se refiere a una búsqueda por nombre? En este sentido, los seudónimos y alias son también relevantes.

- ¿Se trata de un cargo o personaje público? El posible interés público es mayor que en el caso de las personas sin relevancia pública. Como criterio general, hay que valorar si la información vinculada puede descubrir una conducta pública o profesional impropia. En el caso de las personas públicas, sin embargo, debe protegerse la información sobre su salud o su familia. Por tanto, los hechos deben ser relevantes para el debate en una sociedad democrática.

- ¿El interesado es menor de edad? En este caso, la desvinculación debe ser la regla.

- ¿Los datos son correctos? No es lo mismo que la página contenga opiniones del interesado o bien hechos. Se preferirá desvincular resultados de páginas cuya información sea incorrecta o incompleta.

- ¿Son los datos relevantes y no excesivos? Se valorará su relevancia a efectos del interés general. Se tendrá en cuenta, por ejemplo, el tiempo transcurrido: los datos más antiguos no se considerarán tan relevantes como los más actuales. En el caso de ser datos relacionados con la vida laboral del interesado, se protegerán los aspectos más vinculados a la vida privada del interesado y se tenderá a considerar estos irrelevantes a efectos públicos. Si se deniega la desvinculación de injurias o calumnias penales, la autoridad

de control podrá poner los hechos en conocimiento de la fiscalía o de un tribunal competente.

- Los datos especialmente protegidos deberán favorecer la desvinculación.

- Los datos anticuados o no actualizados, sobre todo si producen perjuicio al interesado, deberán obtener una respuesta favorable a su desvinculación.

- Los datos que pueden poner en riesgo al interesado también deberían obtener una respuesta favorable a su desvinculación por parte del responsable.

- El contexto es importante: por ejemplo, puede que se haya intentado, sin éxito, revocar el consentimiento de la publicación original. Si se trata de información en poder de un periódico, en cambio, puede existir justificación legal para organizar la búsqueda por nombres.

- Si la información se refiere a delitos, los de menor entidad y más antiguos pueden ser desvinculados, mientras que los más graves y actuales pueden no serlo. En todo caso, se decidirán caso por caso.

Es importante tener en cuenta, finalmente, la existencia de excepciones o limitaciones al derecho a la supresión o al olvido, que obligan a una ponderación de intereses (art. 17.3 RGPD).

2.2. Derecho a la portabilidad de los datos

Otro derecho nuevo en el Reglamento es el derecho a la portabilidad de los datos cuando el tratamiento se efectúe por medios automatizados (art. 20 RGPD)[13] (Fernández-Samaniego y Fernández-Longoria, 2016, págs. 257-274). Se trata de un complemento al derecho de acceso[14]. De hecho, en un giro copernicano, el interesado se beneficiará del tratamiento de sus datos[15]. Concretamente, el interesado tiene derecho a recibir los datos tratados por un responsable en un formato estructurado, de uso común y lectura mecánica, para poder trasmitirlos a otro responsable. El responsable no podrá oponerse a esta petición del interesado[16] (Fernández-Samaniego y Fernández-Longoria, 2016, pág. 264):

(13)Curiosamente, se ha buscado un antecedente en España con el llamado «derecho a la portabilidad numérica», incluido en el Real Decreto 2296/2004, de 10 de diciembre, por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas, acceso a la red y numeración, que trasponía varias directivas europeas. Se permitía, de acuerdo con el mismo, conservar, de forma gratuita, el mismo número de teléfono, aunque el usuario cambiase de compañía. También existe un *Data Portability Project* de finales del 2007 (www.dataportability.org), con el objetivo de permitir a los usuarios recuperar el control sobre la información. Pese a su impacto limitado, estas iniciativas parecen haber iniciado un debate que ha culminado en el reconocimiento de un auténtico nuevo derecho en el RGPD.

(14)Inicialmente, en la propuesta de RGPD, se encontraba fusionado con el derecho de acceso, como un aspecto de este último. De hecho, la LOPD y su reglamento de desarrollo han ido más allá de la Directiva 95/46/CE, y establecen un derecho de acceso determinando los formatos en los cuales debe entregarse la información al interesado (art. 15 LOPD y art. 28 del RD 1332/2007.

(15)En el considerando 68 del RGPD, se puede leer que la razón de ser de este nuevo derecho es «reforzar aún más el control sobre sus propios datos».

(16)El art. 6 RGPD establece varias condiciones lícitas de tratamiento, de las cuales son de aplicación a la portabilidad el 6.2a –consentimiento explícito sobre los datos especialmente protegidos– y el 6.1b RGPD –contrato en el cual el interesado es parte o aplicación de medidas precontractuales.

- Cuando exista un consentimiento para tratarse para uno o varios fines específicos.
- Cuando el tratamiento es necesario para cumplir un contrato en el cual el interesado es parte.
- Cuando se consiente tratar categorías especiales de datos.
- Cuando el tratamiento se efectúe por medios automatizados[17].

(17)De acuerdo con el art. 20 RGPD, serán tratamientos informatizados que supongan formatos estructurados, de uso común y lectura mecánica.

Por consiguiente, no se ha establecido un derecho general a la portabilidad en supuestos en los cuales el tratamiento no se base en el consentimiento o en un contrato. Por otro lado, cuando sea técnicamente posible, el interesado tendrá derecho a que los datos se transmitan directamente de responsable a responsable. Este derecho no se aplicará cuando el tratamiento obedezca a una finalidad de interés público o en ejercicio de poderes públicos conferidos al responsable. Tampoco podrá el derecho a la portabilidad afectar a los derechos de terceros, ni se hará efectivo cuando los datos solicitados han sido proporcionados al responsable por un tercero.

El grupo del artículo 29 adoptó una guía para concretar los contenidos de este nuevo derecho a la portabilidad (WP29, *Guidelines on the right to data portability*, adoptado el 13 de diciembre del 2016, revisado y adoptado el 5 de abril del 2017, WP 242 rev. 01). Se reconoce la relación entre este derecho y el derecho de acceso, pero difiere por la capacidad de dotar de más poder (*empower*) al interesado para controlar y usar los datos que le conciernen y obran en manos del representante. Otra virtud importante de este derecho es que, al mismo tiempo que protege los derechos del interesado, también mejora la finalidad de libre flujo de datos en el ámbito europeo y promueve la competencia entre responsables. Por tanto, no solo es una medida favorable al interesado, sino

que también sirve a la finalidad pública de promover la competencia y generar nuevos servicios, de acuerdo con la estrategia del mercado único digital europeo. Para el responsable, evidentemente, el nuevo derecho le supone un esfuerzo de interoperabilidad que le obligará a adoptar herramientas informáticas que garanticen que los datos se entreguen en un formato usual, formalizado para su tratamiento automático y que facilite el ejercicio del derecho. Por tanto, un resultado buscado es que el interesado pueda cambiar libremente de proveedor de servicios sin temer perder los datos tras el cambio.

Como complemento al derecho al acceso, el derecho a la portabilidad es, en primer lugar, un derecho a recibir datos personales. Por ejemplo, un sujeto puede tener interés en que su actual proveedor le permita recuperar la lista de música descargada en un servicio de *streaming* musical, para así valorar qué tipo de música quiere contratar en otra plataforma. También puede decidir recuperar su lista de contactos en la aplicación de correo electrónico que usa, para crear una lista de contactos para una boda, por ejemplo. Para hacer efectivo este derecho, sin trabas que desincentiven la portabilidad, el responsable debe prever herramientas automáticas, no solo para que el interesado pueda descargar los datos personales, sino para que puedan transmitirse directamente de responsable actual a responsable futuro. Esto exige una interoperabilidad que se pueda facilitar con API (*application programming interface*), es decir, interfaces y aplicaciones. Evidentemente, el actual proveedor no será responsable del tratamiento de los datos efectuado por el futuro proveedor. Tampoco deberá el responsable retener los datos más allá de lo necesario para su servicio, pensando que algún día un interesado pueda pedir la portabilidad de los datos. Los plazos de retención de los datos no se ven, así, ampliados por el derecho a la portabilidad.

En cuanto al proveedor que recibe los datos, deberá valorar si los datos son relevantes o excesivos para la finalidad del nuevo tratamiento. Por ejemplo, los correos electrónicos recibidos no deberían suponer también el tratamiento de todos los detalles del contacto con los destinatarios. Será necesario valorar su relevancia para el nuevo propósito, y borrar los datos que no sean necesarios. Por consiguiente, la especificación del nuevo propósito debe acompañar el ejercicio del derecho a la portabilidad. También conviene desvincular el ejercicio del derecho a la portabilidad del derecho a seguir recibiendo los servicios del antiguo proveedor, cuando no se sustituya uno por otro, sino que se complementen o se destinen los datos a otro servicio totalmente distinto. Por consiguiente, el ejercicio del derecho a la portabilidad no perjudica los demás derechos del interesado. Así, por ejemplo, si el interesado descubre que los datos facilitados después de ejercer el derecho a la portabilidad no son completos, puede ejercer entonces el derecho de acceso, para verificar los datos completos disponibles.

En cuanto a qué datos se incluyen en el derecho a la portabilidad, el grupo del artículo 29 avanza los siguientes criterios:

a) Los datos personales concernientes al interesado (art. 20.4 RGPD): por consiguiente, todos los datos anónimos o que no sean del interesado no quedan protegidos. En cambio, los seudónimos que estén claramente conectados con el interesado están bajo el amparo del derecho a la portabilidad. En el supuesto de que los datos solicitados contengan también datos de terceros, como datos de terceros destinatarios de llamadas, estos también se facilitarán al interesado. Sin embargo, si los mismos se transmiten a un nuevo proveedor, este último no los procesará para finalidades que puedan afectar a estos derechos de terceros.

b) Los datos proporcionados por el interesado[18]: el derecho a la portabilidad solo puede hacerse efectivo en aquellos supuestos en los que el interesado ha facilitado «directamente» los datos (Fernández-Samaniego y Fernández-Longoria, 2016, pág. 264). Esto incluye no solo los suministrados en formularios en páginas electrónicas, sino también los generados por las actividades del interesado en el uso de un servicio o un aparato: búsqueda histórica en un buscador, datos de conexión y de localización, frecuencia cardíaca recopilada por un aparato de seguimiento de la salud. No se consideran como datos proporcionados por el interesado, en cambio, los datos derivados o creados por el responsable, por ejemplo, mediante programas, a partir de los datos del interesado (art. 27.2 APLOPD): evaluación de capacidad de endeudamiento o evaluación de la salud, personalización o recomendación, categorización o perfil de usuario.

[18]En el derecho de acceso, también se contempla esta diferencia entre los supuestos en que los datos se obtienen directamente del interesado (art. 13 RGPD) y cuando no se han obtenido directamente del interesado (art. 14 RGPD).

c) El ejercicio del derecho a la portabilidad no debe afectar a los derechos de terceros: los datos del interesado que se transfieren al nuevo proveedor lo son mediante consentimiento o contrato. En cambio, los datos de terceros incluidos en la transmisión requieren una cobertura adicional de interés legítimo. Así, si un interesado quiere transmitir a un nuevo proveedor, mediante el derecho a la portabilidad, su directorio de contactos, amigos, conocidos, familiares y grupos, es posible transmitir el directorio entero con los datos de terceros. Estos datos deben estar a disposición solo del interesado, para propósitos personales. En cambio, si los datos de terceros se usaran para finalidades de marketing o promociones de servicios del segundo proveedor, se estarían vulnerando los derechos de información, acceso, cancelación y oposición de los terceros, entre otros. Por lo tanto, en las herramientas de transmisión entre responsables, se deben incluir capacidades de borrado de los datos que no sean necesarios. Finalmente, hay que tener en cuenta que un riesgo para el secreto comercial no es razón suficiente, sin más, para excluir el derecho a la portabilidad.

En cuanto al ejercicio del derecho a la portabilidad, se plantea, en primer lugar: ¿qué información inicial debe dar el responsable al interesado? Es necesario, ante todo, informar precisamente de la existencia del derecho a la portabilidad, de una manera clara y comprensible. Sería útil, según el grupo del artículo 29, distinguir los tipos de datos que puede recibir el interesado mediante el derecho a la portabilidad y el derecho de acceso. Esta información preliminar

debería mencionarse antes del cierre de una cuenta, para que el interesado pueda recopilar los datos y, en su caso, transmitirlos al futuro responsable. Una buena práctica de los responsables receptores consistiría en describir los datos necesarios para su tratamiento. De esta manera, el interesado podría limitar los datos transmitidos. Por otro lado, el responsable debe disponer de herramientas eficaces de identificación del interesado, y cuando el responsable tiene dudas razonables sobre la identidad de un interesado, esto no puede llevar simplemente a negar la solicitar de portabilidad; en efecto, el responsable debe, entonces, requerir información complementaria que le ayude a identificar al interesado. En el caso de seudónimos, el responsable tiene que disponer de herramientas para poder enviar igualmente los datos al interesado. Cuando el volumen de información impida el envío por correo electrónico, el responsable deberá contemplar otras alternativas, como *streaming*, CD o DVD, o la transmisión directa al otro responsable.

La solicitud de portabilidad debe obtener siempre una respuesta que, además, se producirá sin dilaciones indebidas, y en todo caso, en el plazo de un mes desde la recepción de la misma. En los casos complejos, se admite un plazo de hasta tres meses, siempre que se informe de las dificultades al interesado. Si el responsable deniega la solicitud de portabilidad, deberán indicarse las razones por las cuales se ha llegado a esta decisión y las posibilidades de recurrir a una autoridad de control o a un tribunal, siempre en el plazo de un mes desde la recepción de la solicitud. Los motivos para denegar la solicitud son excepcionales, y pueden deberse a su carácter manifiestamente infundado o excesivo y, de manera particular, a su carácter repetitivo. Ahora bien, si el interesado presenta múltiples solicitudes a un responsable, esto no significa que puedan denegarse sin más las mismas cuando no supongan ningún esfuerzo para el responsable. Tampoco podrá repercutirse el coste total de los servicios de respuesta a un interesado, ni ser el motivo por el cual se deniega una solicitud.

Lectura complementaria

Véase al respecto de la solicitud de portabilidad, el WP 242 del grupo del artículo 29.

El formato debe permitir su reutilización, con una estructura que permite su manejo por parte de aplicaciones informáticas, ya sean estas en código abierto o propietario. Los documentos codificados que no puedan ser extraídos fácilmente no son admisibles. Se fomentará el uso de formatos abiertos. Ahora bien, no se establecen formatos concretos en el RGPD, de manera que no se llega a exigir compatibilidad sino, únicamente, interoperabilidad. Para este fin, es necesario disponer de una capa semántica o metadatos que permitan filtrar los datos que no están incluidos en la portabilidad y, a la vez, precisen el contexto y significado de la información efectivamente transmitida. Esta interoperabilidad requiere acuerdos sobre estándares y formatos, en la línea del *european interoperability framework* (EIF) para los servicios públicos. Los datos abundantes o complejos suponen un reto importante, tanto para el responsable como para el interesado. En todo caso, hay que tener en cuenta que la información ha de ser comprensible y manejable. Una manera de hacerlo podría

Lectura complementaria

Véase al respecto de la solicitud de portabilidad, el WP 242 del grupo del artículo 29.

consistir en ofrecer un acceso a los datos mediante una *application programming interface* (API). Esto tendría la ventaja de permitir solicitudes sucesivas o complementarias, solo con los datos actualizados desde la primera solicitud.

Finalmente, el responsable debe garantizar no solo la integridad y confidencialidad de los datos transmitidos, sino también la seguridad de la transmisión misma, por ejemplo, mediante datos encriptados y asegurando que llegan a la persona indicada (se podrían utilizar medidas adicionales de autenticación). Una buena práctica consistiría en recomendar a los interesados un formato y unas medidas de seguridad que permitan a los mismos seguir manteniendo los datos seguros, una vez que estos obran en su poder.

Como todos los derechos, no es absoluto, y se pueden establecer restricciones a partir del Derecho de la Unión o el Derecho nacional[19]. También pueden preverse excepciones a este y otros derechos, sujetas a garantías (art. 89 RGPD y considerando 156). En cuanto a los conflictos con la propiedad intelectual, el responsable no ostenta derechos de propiedad intelectual sobre los datos personales, pero sí podría tenerlos sobre el software con el que los trata en la base de datos[20] (Fernández-Samaniego y Fernández-Longoria, 2016, pág. 271-272).

[19] Considerando 73 del RGPD y art. 23 RGPD: seguridad pública, prevención, investigación y enjuiciamiento de infracciones penales, y otros temas de interés público general.

[20] Esta protección solo es aplicable cuando se ha llevado a cabo una inversión sustancial en el desarrollo de una base de datos, y el responsable deberá valorar la posible infracción de derechos de propiedad intelectual.

2.3. Derecho a no ser objeto de decisiones individuales automatizadas

Este derecho refuerza la protección frente a los perfiles que ya contenía la Directiva 95/46/CE. La sensación era que no se ofrecían unas garantías suficientes, y además se limitaba la previsión a los perfiles obtenidos mediante el seguimiento de los comportamientos del consumidor. En la presente redacción del artículo 22 RGPD, no solo se tienen en cuenta los perfiles, sino que también se amplía su alcance a la elaboración de datos sin seguimiento, puramente mediante técnicas estadísticas sobre datos en bruto. Veamos, pues, el nuevo contenido ampliado.

El interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que tenga efectos jurídicos en él, o le afecte significativamente de modo similar (considerando 71 del RGPD). Más concretamente, el interesado tiene derecho a conocer y que se le comunique la lógica implícita en todo tratamiento automático de datos personales y, al menos en los casos de elaboración de perfiles, las consecuencias del tratamiento (considerando 63 del RGPD). Se establecen, sin embargo, unas excepciones:

- Cuando el tratamiento sea necesario para celebrar o ejecutar un contrato entre el interesado y el responsable.

- Cuando tenga cobertura legal europea o nacional, y se establezcan medidas adecuadas para proteger los derechos del interesado: por ejemplo, en el supuesto de control y prevención del fraude y la evasión fiscal.

- Cuando el interesado consienta explícitamente.

Pese a estas excepciones, el responsable sigue obligado a adoptar medidas adecuadas para salvaguardar los derechos del interesado. En este sentido, como mínimo se garantizará al interesado el derecho a obtener una intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. Como hemos visto anteriormente, el artículo 15 RGPD establece la obligación, en casos de decisiones automatizadas, de proveer información significativa sobre la lógica aplicada, así como la importancia y las consecuencias del tratamiento para el interesado.

Por otro lado, los tratamientos de las excepciones no se basarán en las categorías especiales de datos personales del artículo 9 RGPD (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 la orientación sexual de una persona física), a menos que el interesado haya dado su consentimiento expreso y no exista prohibición para ello; o que el tratamiento sea necesario por razones de interés público esencial. En todo caso, se deberán tomar las medidas adecuadas para preservar los derechos del interesado[21].

(21)La puesta en práctica de este derecho supone un gran reto para la industria y el *big data*, que usa algoritmos como el *machine learning* o, sobre todo, el *deep learning*, supuesto este último en el cual la decisión difícilmente puede explicarse, pues es un estado global de la red neural. En los casos de ontologías jurídicas y de uso de web semántica, parece más fácil de cumplir. Quizá algunas decisiones simplemente no deberían tomarse con herramientas automáticas que no puedan explicar la lógica de su resultado, o limitar, cuando menos, su uso a supuestos que no tengan un efecto significativo sobre los interesados.

2.4. Derecho a la limitación del tratamiento

El interesado puede pedir al responsable la limitación del tratamiento en los siguientes casos (art. 18 RGPD)[22]:

(22)En una versión anterior, este derecho se encontraba en el art. 17, referente al derecho a la supresión o al olvido.

- Cuando impugne la exactitud de los datos, en ejercicio de los derechos de rectificación u oposición, hasta que el responsable lo haya verificado.

- Cuando el tratamiento sea ilícito y el interesado lo solicite en lugar de la supresión de los datos.

- Cuando el responsable no necesite los datos y el interesado, en cambio, sí los quiera para una reclamación.

- Mientras se verifican los motivos legítimos del responsable para no aceptar la solicitud de supresión de los datos.

El efecto de la limitación del tratamiento consiste en que el responsable solo podrá conservar los datos afectados, a menos que obtenga el consentimiento del interesado, en el supuesto de reclamaciones, para proteger derechos o

en interés público. Para resumir, la limitación está prevista en unos supuestos tasados: inexactitud, ilicitud, reclamaciones y, como medida provisional, en caso de no haber ejercido el derecho de supresión, o cuando se ejerce el derecho de oposición mientras se verifica si prevalecen los motivos del representante sobre los del interesado (Álvarez, 2016b, pág. 235). El levantamiento de la limitación por alguno de esto motivos requerirá informar al interesado. Por consiguiente, cuando se ejerzan otros derechos, como el de acceso, los datos no se podrán borrar sin más, pues esto impediría el ejercicio del derecho a la limitación del tratamiento. En cuanto a los métodos para limitar el tratamiento de datos, se mencionan algunos como, por ejemplo, trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, impedir el acceso o en los ficheros automatizados, usando medios técnicos (considerando 67 del RGPD).

3. Limitaciones

El Derecho europeo o nacional podrá limitar el alcance de las obligaciones y derechos del Reglamento (arts. 12 a 22 y 34 RGPD), siempre que se respeten, en lo esencial, los derechos y se trate de medidas necesarias y proporcionadas en una sociedad democrática, en los siguientes casos:

- Seguridad del Estado.
- Defensa.
- Seguridad pública.
- Prevención e investigación de delitos o sanciones penales.
- Protección de objetivos de interés público.
- Protección de la independencia judicial.
- Prevención e investigación de infracciones de normas deontológicas en profesiones reguladas.
- Protección de derechos de otros.
- Ejecución de demandas civiles.

Con el fin de evitar que estas limitaciones acaben socavando de raíz los derechos reconocidos en el Reglamento, se contemplan unos contenidos garantistas que las medidas deberán respetar. Así, la medida limitadora deberá especificar:

- La finalidad del tratamiento.
- Las categorías de datos afectadas.
- El alcance de las limitaciones.
- Las garantías para evitar accesos o transferencias de datos ilícitos o abusivos.
- El responsable o categorías de responsables.

- Los plazos de conservación y las garantías previstas de acuerdo con su naturaleza, la finalidad del tratamiento o el tipo de tratamiento.

- Los riesgos respecto a los derechos.

- El derecho del interesado a ser informado sobre la limitación, a menos que ello pudiera perjudicar los fines de la misma.

Bibliografía

AEPD (2016). *Guía para el cumplimiento del deber de informar*.

Álvarez, M. (2016a). «El derecho a la supresión o al olvido». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 241-256). Madrid: Ed. Reus.

Álvarez, M. (2016b). «El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 227-256). Madrid: Ed. Reus.

Fernández-Samaniego, J.; Fernández-Longoria, P. (2016). «El derecho a la portabilidad de los datos». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 257-274). Madrid: Ed. Reus.

Grupo de trabajo del artículo 29 de la Directiva 95/46/EC (2016, 13 de diciembre). *Guidelines on the right to data portability*. WP 242.

Hernández, J. A. (2016). «Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 205-226). Madrid: Ed. Reus.

López, M. (2014). «Derecho a la información y derecho al olvido en Internet». *La Ley Unión Europea* (núm. 17, julio).

Pazos Castro, R. (2015). «El mal llamado derecho al olvido en la era de Internet». *Boletín del Ministerio de Justicia* (núm. 2183, noviembre, año LXIX).

Peguera, M. (2015). «In the Aftermath of Google Spain: How the 'Right to Be Forgotten' is Being Shaped in Spain by Courts and the Data Protection Authority». *International Journal of Law and Information Technology* (vol. 23, núm. 4, págs. 325-347). doi: 10.1093/ijlit/eav016.

Peguera, M. (2016). «The Shaky Ground of the Right to Be Delisted». *Vanderbilt Journal of Entertainment & Technology Law* (vol. 18, núm. 3, págs. 507-561).

Touriño, A. (2014). *El derecho al olvido y a la intimidad en Internet*. Madrid: La Catarata.

Troncoso, A. (2010). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant lo Blanch.

Troncoso, A. (2013). «Las redes sociales a la luz de la Propuesta de Reglamento general de Protección de Datos Personales». *Revista de Internet, Derecho y Política* (núm. 16, junio). Barcelona: Universitat Oberta de Catalunya.