La protección de datos personales en la administración pública

PID_00253422

Agustí Cerrillo Martínez

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Índice

Introducción

Las tecnologías de la información y la comunicación están suponiendo nuevas amenazas para los datos personales. A continuación se presentarán las medidas que el derecho está adoptando para poder proteger los datos de las personas frente a los ataques que pueden provenir de Internet.

Esta introducción se articulará en dos ámbitos. Por un lado, se verá, en general, cuál ha sido la regulación de la protección de los datos personales. Y por otro lado, cuál es el impacto del desarrollo de la administración electrónica en la protección de los datos personales.

Objetivos

Los objetivos del presente módulo son:

1. Conocer la regulación de la protección de datos personales.

2. Analizar los distintos usos de los medios electrónicos en la administración pública desde la perspectiva de la protección de los datos personales.

3. Valorar el impacto de la protección de datos personales en el desarrollo de la administración electrónica.

1. La regulación de la protección de datos personales

Lectura propuesta

A. Troncoso Reigada (2008). "La administración electrónica y la protección de datos personales". *Revista Jurídica de Castilla y León*. <http://www.navarra.es/NR/rdonlyres/E6188543-88F9-476F-8581- 406069D3C0E7/188896/32 Administracionelectronicay protecciondedatosTronc.pdf>

a) ¿Cuáles son los peligros de la extensión de las tecnologías de la información y la comunicación para las personas?

La Constitución española reconoce el derecho a la intimidad, que implica, como ha reconocido el Tribunal Constitucional, la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario para mantener una calidad mínima de la vida humana. Además, también prevé el derecho a la protección de los datos de carácter personal que garantiza a los individuos un poder de disponer de ellos y controlarlos.

Pagar los impuestos por Internet o cumplimentar un formulario para solicitar una subvención a una administración pública son dos actividades que, más allá de poner en contacto a un ciudadano con una administración para cumplir un deber o conseguir un bien o un servicio, ponen en circulación en Internet datos personales (nombre y apellidos, dirección, número de documento de identidad, número de la tarjeta de crédito o de la cuenta corriente). En muchos casos estos datos pueden parecer insignificantes o podemos no darles importancia porque no los consideramos secretos o no afectan a lo que consideramos la propia intimidad.

La utilización de los medios electrónicos puede facilitar la vulneración de la intimidad de las personas. Las TIC permiten acceder y agregar datos personales dispersos que de este modo facilitan un perfil de la persona afectada, lo cual era difícilmente realizable, o tenía costes muy elevados, sin utilizarlas. También permiten poder conocer las actividades realizadas al navegar por Internet, si se visita una página u otra o si se compra un producto u otro. Todo eso sin que la persona afectada tenga conocimiento y sin dejar rastro alguno. De este modo, no puede ejercer ningún control sobre estos datos ni sobre el uso que se hace de los mismos.

Así, por ejemplo, se puede llegar a la situación de que, a partir de los pagos que se hacen actualmente mediante la tarjeta de crédito, fácilmente se puede obtener una lista de los productos adquiridos que proporcione una idea del perfil de cliente que es, algo muy interesante para muchas empresas que quieren saber cuáles son las preferencias de clientes potenciales.

Esta situación ha sido claramente descrita en la STC 292/2000, de 30 de noviembre, al afirmar lo siguiente:

"Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no solo cuáles son los datos que le conciernen que se hallan recogidos en un fichero, sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí solo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico".

Frente a los riesgos que la generalización del uso de las TIC puede suponer para la intimidad de las personas, se han adoptado distintas regulaciones que tienen por objeto establecer normas para regular el tratamiento de datos personales y también se han creado autoridades de control del cumplimiento de dichas normas.

El artículo 18.4 CE establece que la "ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

El Tribunal Constitucional ha reconocido la existencia de un derecho a la autodeterminación informativa o de una libertad informática. Este derecho fue reconocido por primera vez por el Tribunal Constitucional alemán en la sentencia de 15 de diciembre de 1983 sobre la Ley del censo. En dicha sentencia, el Tribunal Constitucional alemán consideró el derecho a la autodeterminación informativa en base al derecho a la autodeterminación de la persona e identificó este nuevo derecho, que implica que cada individuo puede decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida. Para el Tribunal Constitucional alemán, el libre desarrollo de la personalidad presupone, en las condiciones modernas de la elaboración de datos, la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitados de los datos referentes a la persona. Así, tal como afirma en el fundamento jurídico segundo:

"[...] en la clave de bóveda del ordenamiento de la Ley fundamental se encuentra el valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre. El derecho general de la personalidad abarca la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida: la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos de protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona.

El derecho fundamental garantiza, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y utilización de sus datos personales[1]".

(1)http://www.informatica-juridica.com/jurisprudencia/alemania.asp

De todos modos, hay que poner de manifiesto que el derecho a la autodeterminación informativa no es un derecho absoluto, por lo que tiene que ser ponderado con otros derechos o intereses que en un momento dado se consideran de prioritaria atención.

"Las limitaciones de este derecho a la «autodeterminación informativa» solo son admisibles en el marco de un interés general superior y necesitan un fundamento legal basado en la Constitución que tienen que corresponder al imperativo de claridad normativa inherente al estado de derecho[2]".

(2)STC alemán de 15 de diciembre de 1983.

b) ¿Cuál es el contenido que el Tribunal Constitucional ha dado al derecho a la protección de los datos personales?

La jurisprudencia del Tribunal Constitucional ha permitido delimitar el contenido del derecho previsto en el artículo 18.4 CE. Así, por ejemplo, la STC 254/1993, de 20 de julio:

> "En efecto, hay que tener presente, como ya se anticipaba en la decisión de este Tribunal que se acaba de mencionar, que el derecho fundamental al que hacemos referencia garantiza a la persona un poder de control y disposición sobre sus datos personales, puesto que confiere a su titular todo un abanico de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir que se recojan y utilicen sus datos personales y a conocerlos. Y para hacer efectivo dicho contenido, otorga el derecho a ser informado sobre quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esta posesión y uso exigiendo a quien corresponda que se ponga fin al mismo.
>
> En suma, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a los que sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De forma que es en estos ficheros donde tienen que proyectarse, en última instancia, las medidas destinadas a la salvaguarda del derecho fundamental aquí considerado por parte de las administraciones públicas competentes".

c) ¿Cuáles son las relaciones entre el derecho a la intimidad y el derecho a la protección de los datos personales?

La STC 292/2000, de 30 de noviembre, permite distinguir claramente entre el derecho a la intimidad y el derecho a la autodeterminación informativa:

> "6. La función del derecho fundamental a la intimidad del artículo 18.1 CE es proteger frente a cualquier invasión que se pueda realizar en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (para todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esta persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir el tráfico ilícito y lesivo para la dignidad y derecho del afectado. En conclusión, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno; por esta razón, y así lo ha manifestado este Tribunal (STC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de proteger su vida privada de una publicidad no deseada. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre dichos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esta información sin las debidas garantías, así como el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidos de tal información. Pero este poder de disposición sobre los propios datos personales no tiene ningún valor si el afectado desconoce qué datos poseen terceros, quién los posee y con qué finalidad.
>
> De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, tanto si es íntimo como si no lo es, cuyo conocimiento o uso por parte de terceros pueda afectar a sus derechos, tanto si son fundamentales como si no lo son, porque su objeto no es solo la intimidad individual, que para eso está la protección que otorga el artículo 18.1 CE, sino los datos de carácter personal[3]".

(3)Véase también la STC 143/1994, de 9 de mayo, FJ 7.

De acuerdo con el TC, la distinción entre los dos derechos se concreta, por un lado, por el objeto que tiene y, por otro, por el contenido.

En cuanto al objeto, el artículo 18.4 CE es más amplio que el derecho a la intimidad, puesto que no se limita a los datos íntimos de las personas, sino que extiende la garantía a cualquier tipo de datos personales, tanto íntimos como no, cuyo conocimiento por parte de terceros pueda afectar a los derechos de la persona.

En cuanto al contenido, el artículo 18.1 CE confiere al titular un poder jurídico para imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo que haya sido conocido mediante una intromisión y, en cambio, el derecho de protección de datos atribuye al titular un conjunto de facultades consistente en distintos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que sirven a la función que realiza el derecho en cuanto a la protección de datos: garantizar a la persona un poder sobre sus datos personales.

d) ¿Cómo se ha regulado la protección de los datos personales?

El movimiento regulador tiene su origen en el ámbito estatal. La primera ley sobre protección de datos fue aprobada en el *Land* alemán de Hessen en 1970. Posteriormente, otros estados como Suecia, Estados Unidos, Nueva Zelanda, Canadá y gran parte de los países europeos se han dotado de instrumentos legislativos en esta materia.

Gran parte de este movimiento ha tenido su origen en las regulaciones promovidas internacionalmente. En primera instancia, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, de protección de las personas en relación con el tratamiento automatizado de los datos de carácter personal. El objetivo del Convenio es asegurar en el territorio de los estados firmantes que se respete el derecho de cada individuo, independientemente de su nacionalidad o residencia, a la privacidad respecto al proceso automatizado de los datos personales que se refieren al mismo.

Posteriormente, en el ámbito comunitario, se aprobó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas, y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. En mayo de 2003, se adoptó un informe sobre la aplicación de la Directiva 95/46, de acuerdo con lo que se establece en el artículo 33. En dicho informe se constató que la Directiva 95/46 había logrado el objetivo de otorgar una protección suficiente de la privacidad y que, al mismo tiempo, había facilitado la transferencia de datos a la Unión Europea. Sin embargo, la tardanza en la implementación de la Directiva por parte de algunos estados miembros y también las diferencias en su transposición han motivado que la economía europea no se haya beneficiado completamente de la Directiva[4].

[(4)]Véase el informe en: http://eur-lex.europa.eu/lexuriserv/lexuriserv.do?uri=celex:52003DC0265:SE:NOT.

Ejemplo

Tal como recuerda la Sentencia del Tribunal de Justicia de la Unión Europea de 20 de mayo de 2003 en los asuntos acumulados C-465/00, C-138/01 y C-139/01, la Directiva 95/46, "adoptada sobre la base del artículo 100 A del Tratado, tiene por objeto garantizar la libre circulación entre estados miembros de los datos personales mediante la armonización de las normas nacionales que protegen a las personas físicas en cuanto al tratamiento de estos datos". En efecto, el artículo 1 de la citada Directiva, que define su objeto, dispone, en su apartado 2, que los estados miembros no pueden restringir ni prohibir la libre circulación de datos personales entre los estados miembros por motivos relacionados con la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en cuanto al tratamiento de estos datos.

En 2016 se ha aprobado el 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) que tiene efecto directo sin necesidad de ser transpuesto.

El RGPD introduce importantes novedades en materia de protección de datos que tienen una incidencia especial en las administraciones públicas.

Véase en síntesis el documento:

Agencia Española de Protección de Datos (2017). *El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Públicas*.

<https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf>

La legislación europea ha sido transpuesta al ordenamiento jurídico español mediante la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), y, en determinados aspectos, mediante la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información (LSSI). La LOPD derogó la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

Además, tres comunidades autónomas han adoptado algunas normas sobre tal cuestión. La Comunidad de Madrid fue la primera comunidad autónoma en aprobar una ley en esta materia, en particular la Ley 8/2001, de 13 de julio, de protección de datos de carácter personal en la Comunidad de Madrid, que tiene por objeto regular los ficheros de datos de carácter personal y la Agencia de Protección de Datos de la Comunidad de Madrid. Posteriormente, la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, que como se desprende de su título crea y regula la Agencia Catalana de Protección de Datos (en la actualidad, Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos). Finalmente, el País Vasco aprobó la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, con el objetivo de regular los ficheros de datos de carácter personal creados o gestionados por

la Comunidad Autónoma del País Vasco, los órganos forales de los territorios históricos y las administraciones locales de la Comunidad Autónoma del País Vasco, y crear y regular la Agencia Vasca de Protección de Datos.

Además de todas estas normas que directamente inciden en los datos de carácter personal y tienen por objeto único y específico la protección de los mismos, cabe poner de relieve otras normas de carácter general que inciden en esta materia. Son normas como el Código penal y el Código civil, o la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y el comercio electrónico (LSSI), a la cual hay que hacer una particular mención.

También hay que poner de relieve que en determinados ámbitos se ha optado por adoptar códigos de conducta, es decir, mecanismos de autorregulación por parte del propio sector que implican que aquellos que se acogen a los mismos se obligan a seguir las reglas de conducta que se establecen. La LOPD contempla la posibilidad de formular códigos tipo a los responsables de ficheros, a través de acuerdos sectoriales o decisiones de empresa. En particular, el artículo 32 LOPD determina que los responsables de tratamientos de titularidad pública y privada pueden formular códigos que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías para el ejercicio de los derechos de las personas. Los códigos tipo tienen el carácter de códigos deontológicos o de buena práctica profesional y tienen que depositarse e inscribirse en el Registro General de Protección de Datos.

e) ¿Cómo se garantiza el cumplimiento de la legislación sobre protección de datos personales?

La Agencia Española de Protección de Datos es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las administraciones públicas en el ejercicio de sus funciones. Entre sus funciones destacan:

- Velar por el cumplimiento de la legislación sobre protección de datos y controlar la aplicación, especialmente en cuanto a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

- Atender las peticiones y reclamaciones de los afectados.

- Emitir las autorizaciones que establece la Ley, ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos, ejercer la potestad sancionadora, y pedir la ayuda e información que precise.

- Informar de los proyectos de normas de desarrollo que incidan en materia de protección de datos.

Para conseguir tales fines, la propia Ley reconoce toda una serie de potestades, como son las de investigación e inspección para obtener información y, si procede, pruebas sobre los hechos que contravengan lo que dispone la Ley, la potestad sancionadora, que la Agencia de Protección de Datos tiene que ejercer en los términos que determina la Ley, la potestad de resolución de las reclamaciones de los afectados por incumplimiento de las previsiones de la citada Ley y la potestad normativa, ceñida en lo esencial a dictar las instrucciones necesarias para adecuar los tratamientos automatizados a los principios de la LOPD.

La STC 290/2000 es clara al definir el carácter de las funciones de la Agencia Española de Protección de Datos:

> En efecto, puesto que da cumplimiento al mandato que contiene el artículo 18.4 CE, el legislador, sin excluir de ninguna forma el recurso último a los órganos jurisdiccionales para la tutela de los derechos individuales, como se determina en los apartados 2 a 5 del artículo 17 LORTAD, no ha querido aun así que la protección de datos personales frente al uso de la informática se lleve a cabo exclusivamente en la vía judicial, esto es, cuando ya se ha producido una lesión del derecho fundamental. Al contrario, ha querido que esta protección se lleve a cabo mediante el ejercicio por la Agencia de Protección de Datos, con carácter básicamente preventivo, de las funciones de control de los ficheros tanto de titularidad pública como privada que la LORTAD le atribuye y, si procede, a través de las reclamaciones de los afectados ante la Agencia de Protección de Datos (art. 17.1), que provocarán la posterior actuación de dicho órgano.

En esta sentencia los recurrentes consideran que, al limitar las competencias autonómicas a los ficheros automatizados de datos de carácter personal creados o gestionados por ellas, se vulneraba el sistema de distribución de competencias, puesto que a consecuencia de dicha limitación corresponde en exclusiva a un órgano estatal, la Agencia de Protección de Datos, la ejecución de la Ley y el ejercicio de las funciones interventoras y sancionadoras que se contemplan respecto al resto de ficheros automatizados. El Tribunal Constitucional considera que "es la garantía de los derechos fundamentales exigida por la Constitución, así como la de la igualdad de todos los españoles en su disfrute, la que en este caso justifica que la Agencia de Protección de Datos y el Registro Central de Protección de Datos puede ejercer las funciones y potestades a que antes se ha hecho referencia respecto a los ficheros informatizados que contengan datos personales y que sean de titularidad privada radicados en Cataluña".

En Cataluña, en 2003, se creó la Agencia Catalana de Protección de Datos, que, como recoge su ley de creación, tiene por objeto velar por el respeto de los derechos fundamentales y las libertades públicas de los ciudadanos en lo concerniente a las operaciones realizadas mediante procesos automatizados o manuales de datos personales.

En Madrid, la Agencia de Protección de Datos de la Comunidad de Madrid tiene como finalidad garantizar y proteger los derechos fundamentales de las personas físicas respecto al honor y la intimidad familiar y personal, en cuanto al tratamiento de sus datos personales. Sus competencias versan sobre los

ficheros de titularidad pública creados o gestionados por la Comunidad Autónoma de Madrid, ente que integra a la Administración local de su ámbito territorial, universidades públicas y corporaciones de derecho público representativas de intereses económicos y profesionales de aquella. A pesar de la intensa actividad desarrollada desde su creación, la Agencia de Protección de Datos de la Comunidad de Madrid fue suprimida en 2012.

En el País Vasco, la Agencia Vasca de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones, entre las cuales destacan velar por el cumplimiento de la legislación sobre protección de datos y controlar la aplicación y emitir las autorizaciones previstas en las leyes y los reglamentos.

f) ¿Qué es un dato personal?

La primera cuestión que hay que delimitar es la relativa a qué se entiende por *dato*. De la legislación española de protección de datos se pueden extraer las siguientes consideraciones de carácter general. La LOPD, siguiendo la Directiva 95/46, parte de una definición amplia de los datos personales: "Cualquier información concerniente a personas físicas identificadas o identificables".

Identificada o identificable es toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. En relación con este concepto se plantean algunas dudas, entre las que destaca si se pueden considerar las personas jurídicas como titulares de los derechos reconocidos en la LOPD. Teniendo en cuenta que el artículo 18.4 CE se refiere a los ciudadanos y que la Directiva 95/463 hace referencia a la protección de las personas físicas, parece ser que hay que concluir en sentido negativo. Sin embargo, si los datos referidos a una persona jurídica se pueden atribuir a una persona física concreta, aunque fueran tratados como datos de una persona jurídica, tendrían la consideración de datos de carácter personal.

Los datos de carácter personal no son únicamente información numérica o alfanumérica, sino que también hay que entender que hacen referencia a la imagen, la voz, las huellas dactilares o los datos biométricos. Estos datos no tienen que estar únicamente en ficheros automatizados. A diferencia de la LORTAD, la LOPD considera que la norma es aplicable a los datos de carácter personal registrados en soporte físico.

El uso de las nuevas tecnologías plantea si determinada información puede considerarse como dato de carácter personal. En particular, la pregunta sería si la dirección electrónica y la dirección IP son datos de carácter personal. En cuanto a la dirección electrónica, si tenemos en cuenta que para considerar que estamos frente a un dato personal es preciso que haya una vinculación

entre la información y la persona concreta, la dirección electrónica no debería considerarse un dato de carácter personal mientras no exista tal relación. En cuanto a la dirección IP, la Agencia Española de Protección de Datos considera que es un dato de carácter personal:

> "Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP, tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos[5]".

(5)Informe 327/03.

g) ¿Qué son los principios de la protección de datos?

La LOPD establece toda una serie de principios:

Calidad de los datos. Los datos personales tienen que ser adecuados, pertinentes y no excesivos respecto a la finalidad para la cual se obtienen y tienen que ser exactos y actualizados. Se trata de asegurar la veracidad y exactitud de los datos obtenidos y tratados. Como afirma la Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 9 de marzo de 2001:

> "Uno de los principios que inspira la legislación sobre tratamiento automatizado de datos de carácter personal es el de calidad de datos. Este principio implica, entre otras cosas, que los datos sean necesarios y pertinentes para la finalidad para la cual se hayan recogido o registrado (art. 4.5 de la LO 5/1992) y que sean exactos y completos (art. 4.4 de la LO 5/1992). Por lo tanto, si los datos han dejado de ser necesarios para las finalidades para las que se han recogido o registrado o son inexactos, hay que proceder [...] a cancelarlos, sin necesidad de solicitarlo al afectado. Y así se infiere del mismo tenor literal de los artículos 4.4 y 4.5 de la LO 5/1992, que utiliza la expresión imperativa «tienen que ser cancelados» y sin condicionarla a la existencia de una solicitud previa del afectado. En suma, la norma establece la obligación del responsable del fichero de proceder de oficio y con la debida diligencia a cancelar los datos inexactos o que han dejado de ser necesarios para la finalidad del fichero y sin necesidad de solicitud previa del afectado".

Consentimiento. El tratamiento de los datos de carácter personal requiere el consentimiento inequívoco del interesado. La Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 29 noviembre de 1999, afirma sobre dicha cuestión lo siguiente:

> "[...] El precepto establece no solo el uso de los datos sino el tratamiento [...]. Pues bien, este tratamiento tiene que respetar, entre otras garantías previstas por la Ley, la que establece el artículo 6, apartados 1 y 2, que exigen para el tratamiento de los datos el consentimiento del afectado, consentimiento que no es necesario cuando los datos de carácter personal se recojan de fuentes accesibles al público. La infracción de dicha garantía es la que se imputa concretamente a la actora, estableciéndose ya desde el pliego de cargos que los datos no se han obtenido con el consentimiento del interesado ni provienen de fuentes accesibles al público".

Existen datos (ideología, afiliación sindical, religión y creencias) que tienen una protección reforzada y que requieren un consentimiento expreso y por escrito. Otros datos (origen racional, salud o vida sexual) solo pueden ser recogidos, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado lo consienta expresamente.

En relación con el principio del consentimiento, existe el de la plena información del afectado, respecto al cual se puede traer a colación la Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 15 de junio de 2001:

> "En primer lugar, hay que tener en cuenta que nos encontramos frente a la regulación del derecho de información a la recogida de datos, derecho importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos, y así lo valora el texto positivo al pormenorizar su contenido y establecer la exigencia de que el mismo sea expreso, preciso e inequívoco. La relevancia del derecho comporta que su exclusión requiera el mandato expreso de una norma, acogiendo una interpretación estricta, vetando su extensión mediante artificiosas deducciones".

Seguridad de los datos. De acuerdo con el artículo 9 LOPD, "el responsable del fichero y, en su caso, el encargado del tratamiento deben adoptar las medidas de carácter técnico y organizativo necesarias que garanticen la seguridad de los datos de carácter personal y eviten la alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana como del medio físico o natural".

Secreto en el tratamiento de los datos. El responsable del fichero y del tratamiento está obligado al secreto profesional. De acuerdo con la Sentencia de la Sección Novena de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 3 de mayo de 2001:

> "[...] el deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto solo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga la persona a que se refiera la información. En este caso [...] la repercusión para el afectado de la divulgación de datos a terceros es sumamente subjetiva, de tal forma que, en el supuesto que nos ocupa, podría afectar más a la interesada la comunicación de su deuda a su padre que a cualquier otra persona".

Congruencia y racionalidad en su utilización. Así, el artículo 11 LOPD establece que "los datos de carácter personal objeto del tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de finalidades directamente relacionadas con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado".

h) ¿Cuáles son los derechos de las personas respecto a los datos personales?

Para garantizar el cumplimiento de estos principios, la LOPD regula los derechos de los titulares de los datos personales y los tratamientos que pueden realizarse:

Derecho de acceso. El interesado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de los datos y las comunicaciones realizadas o que se prevean realizar.

En la Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 17 de mayo de 2000, se afirmó lo siguiente:

> "El derecho de acceso es el derecho a solicitar y obtener información de los datos de carácter personal incluidos en los ficheros automatizados [...] Y fue precisamente la falta de respuesta de la petición de información del denunciante [...] en el plazo de un mes [...] la que motivó la incoación de un procedimiento de tutela del derecho de acceso del denunciante, cuya finalidad no era otra que la de dar efectividad a tal derecho [...] al no haber sido satisfecho por el titular del fichero [...]".

Derecho de rectificación y cancelación. Deben ser rectificados o cancelados, si procede, los datos de carácter personal cuando el tratamiento no se ajuste a lo que dispone la LOPD. En este sentido, la Sentencia de la Sección Novena de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 17 de junio de 1999, recoge lo siguiente:

> "[...] el responsable del fichero es quien [...] tiene la obligación de hacer efectivo el derecho de rectificación y cancelación [...] La Instrucción 1/98 ha sido aclaratoria, puesto que impone al responsable del fichero la obligación de tomar medidas para trasladar la solicitud que se efectúe de cancelación o rectificación, a la entidad bancaria suministradora del dato, de forma que, si no recibe respuesta en cinco días, tiene que proceder a la rectificación cautelar de los ficheros".

Derecho de oposición. Se reconoce en dos preceptos de la LOPD, los artículos 6.4 y 30.4. El primero reconoce el derecho del interesado que tenga un interés legítimo a oponerse al tratamiento de sus datos en aquellos supuestos en que, de acuerdo con lo que establece el artículo 6.2, no haya que pedirle el consentimiento, e indica que "en los casos en que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, este podrá oponerse a su tratamiento cuando existan motivos fundamentados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero debe excluir del tratamiento los datos relativos al afectado".

El segundo reconoce el llamado *derecho de opt-out*, o derecho a no ser incluido en las listas obtenidas de fuentes accesibles al público y empleadas con fines de publicidad o prospección comercial, y establece que "los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquel, a su simple solicitud".

La misma LOPD contempla algunas excepciones a los derechos anteriores. En particular, el artículo 23 LOPD establece, entre otros, que "los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o la cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y las libertades de terceros o las necesidades de las investigaciones que se estén realizando".

La Agencia Española de Protección de Datos es competente respecto a la tutela del derecho de acceso que corresponde a cada persona y deriva de su derecho a la privacidad de sus datos de carácter personal. Así, ante una denegación del ejercicio de este derecho, queda abierta la posibilidad de pedir esta tutela formulando la correspondiente reclamación.

i) ¿Cómo se pueden obtener los datos?

La LOPD contempla distintos mecanismos para la obtención de los datos:

Obtención de datos del propio interesado

En primer lugar, la obtención puede ser a través de la persona que, o bien los ha facilitado directamente, o bien manifiesta el consentimiento expreso para que sean recogidos con una finalidad concreta y, por lo tanto, no genérica. El suministro de datos puede ser voluntario o fruto de una obligación legal (por ejemplo, los datos necesarios para el empadronamiento).

De acuerdo con la LOPD, "los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos". Por eso hay que entender que el consentimiento se da respecto a un tratamiento que tiene una finalidad concreta. No es un consentimiento abstracto, sino para un tratamiento o unos tratamientos concretos. El consentimiento tiene que ser inequívoco a través de una manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consienta el tratamiento de los datos personales que le conciernen.

Tal como se ha observado anteriormente, existen determinados casos en los que la LOPD exige consentimiento reforzado para tratar determinados datos debido al carácter especialmente sensible de los mismos. Además, en relación con los datos sobre ideología, religión o creencias, hay que advertir al interesado sobre el derecho a no prestar el consentimiento. Es interesante poner de relieve que respecto a tales datos no es preciso el consentimiento cuando el tratamiento sea necesario para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios o para salvaguardar el interés vital del afectado o de otra persona, en caso de que el afectado esté física o jurídicamente incapacitado para dar el consentimiento.

Aunque se haya prestado el consentimiento, este es revocable cuando exista una causa justificada y no se le atribuyan efectos retroactivos.

La LOPD establece algunas excepciones a la necesidad del consentimiento. En primer lugar, cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las administraciones públicas, en el ámbito de sus competencias. En segundo lugar, cuando se refieran a las partes de un contrato

o precontrato de una relación de negocios, laboral o administrativa y sean necesarias para su mantenimiento o cumplimiento. En tercer lugar, cuando el tratamiento tenga por finalidad proteger un interés vital del interesado. Y, en cuarto lugar, cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y las libertades fundamentales del interesado.

Obtención de datos de fuentes diferentes al interesado

La obtención de datos de fuentes distintas al interesado puede ser a través de fuentes accesibles al público, como por ejemplo los censos promocionales, los repertorios telefónicos o las listas profesionales o como resultado de la cesión de datos personales de sujetos distintos al interesado.

Como punto de partida en este supuesto hay que traer a colación el artículo 5.4 LOPD, que establece que cuando los datos no se obtengan del interesado debe informase, de forma expresa, precisa e inequívoca, dentro de los tres meses siguientes al momento de registro de los datos, del contenido del tratamiento, procedencia de los datos y del resto de aspectos que prevé la Ley.

De acuerdo con la LOPD, son fuentes accesibles al público "los ficheros que pueden ser consultados por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación". Tienen la consideración de fuentes de acceso público el censo promocional, los repertorios telefónicos y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al público. También tienen la consideración de fuentes de carácter público los diarios y boletines oficiales y los medios. A pesar de que los datos se obtengan de una fuente, no pueden someterse a cualquier tipo de tratamiento. Es preciso que el tratamiento de los datos sea necesario para la satisfacción de un interés legítimo del responsable del fichero o del tercero a quien se comuniquen los datos, y que se cumpla la condición de no vulnerar los derechos y las libertades fundamentales del afectado.

Para la cesión de datos es necesario que estos sirvan para el cumplimiento de finalidades directamente relacionadas con las funciones legítimas del cedente y del cesionario y el consentimiento previo del interesado. Sin embargo, están previstas distintas excepciones a la regla del consentimiento previo. La comunicación de datos entre administraciones públicas estaba prevista en el artículo 21 LOPD, que fue declarado inconstitucional por la STC 292/2000, de 30 de noviembre.

j) ¿Cómo deben crearse los ficheros de datos personales?

Tanto las administraciones públicas como los particulares pueden crear ficheros que contengan datos personales. Los requisitos en un caso y otro son distintos pero tienen en común la necesidad de inscribir el fichero en el Registro General de Protección de Datos creado a tal efecto en la Agencia Española de Protección de Datos.

Los ficheros de titularidad pública. Los ficheros de titularidad pública comprenden los de las administraciones públicas u otros entes, organismos o corporaciones de derecho público. Solo se pueden crear, modificar o suprimir por medio de una disposición general publicada en el BOE o en el diario oficial correspondiente. Una vez creado el fichero, la Administración o el organismo responsable tiene que comunicarlo a la Agencia Española de Protección de Datos para la inscripción en el Registro General de Protección de Datos.

La LOPD regula la recogida y el tratamiento de datos para finalidades policiales sin el consentimiento de las personas afectadas. Respecto a los ficheros de las fuerzas y cuerpos de seguridad, se establecen una serie de excepciones a los derechos de acceso, rectificación y cancelación, y también la limitación de derechos como el de información al afectado.

El RGPD dispone que las Administraciones públicas deben llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

Este registro debe contener la siguiente información:

a) el nombre y los datos de contacto del responsable y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional;

f) los plazos previstos para la supresión de las diferentes categorías de datos;

g) una descripción general de las medidas técnicas y organizativas de seguridad.

El registro podrá organizarse sobre la base de las informaciones ya proporcionadas en las notificaciones de los ficheros existentes. Las Administraciones públicas deberán mantener el registro actualizado.

El registro se pondrá a disposición de la autoridad de control que lo solicite.

Los ficheros de titularidad privada. De acuerdo con la LOPD, son ficheros de titularidad privada los que contengan datos de carácter personal cuando, de forma acumulativa, sea necesario para la consecución de la actividad u objeto legítimo de la persona, empresa o entidad titular y se respeten las garantías que la LOPD establece para la protección de las personas. La creación de ficheros de titularidad privada tiene que ir precedida por la notificación a la AEPD. El Registro General de Protección de Datos procede a la inscripción del fichero si la notificación se ajusta a los requisitos exigibles. Esta puede ser concedida por silencio administrativo. La LOPD hace una regulación específica de algunos ficheros de titularidad privada:

- Ficheros que contienen datos de solvencia patrimonial. La cesión de información relativa a la solvencia patrimonial tiene una excepción al consentimiento del afectado, que está motivada por razones de interés público representado en la protección del interés público.

- Ficheros con finalidad de publicidad y prospección comercial. Se regula especialmente el origen de los datos y el derecho de los afectados a conocerlo. En relación con estos datos propios de lo que se conoce como *marketing relacional* es de interés tener en cuenta que la LSSI regula las comunicaciones comerciales por vía electrónica (arts. 19-22). Finalmente, hay que señalar que la LOPD regula el censo promocional elaborado por el Instituto Nacional de Estadística u órgano equivalente de las comunidades autónomas con una vigencia anual, que estará formado por los datos de nombre, apellidos y domicilio que constan en el censo electoral.

k) ¿Cómo debe garantizarse la seguridad de los datos?

Bajo este título se incluyen operaciones tan diversas como los mecanismos de seguridad y secreto de los datos hasta su consulta y acceso y, si procede, su rectificación o cancelación. Los responsables de los ficheros tienen la obligación de garantizar la seguridad y guardar el secreto profesional de los datos a los cuales tienen acceso. En cuanto a los titulares de los datos, tienen derecho a acceder de forma gratuita a la información sobre sus datos de carácter personal y el derecho a rectificar y cancelar los datos de un fichero. También tienen derecho de amparo y de indemnización.

Seguridad de los datos. El responsable del fichero y el encargado del tratamiento tienen el deber de adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y evitar la alteración, pérdida, tratamiento o acceso no autorizado, según el estado

de la tecnología, la naturaleza de los datos y los riesgos a que estén expuestos. Para garantizar la seguridad no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones determinadas reglamentariamente. La finalidad de las medidas de seguridad es la de garantizar la confidencialidad (permitir el conocimiento de los datos solo a los usuarios autorizados), integridad (impedir la alteración de la información) y disponibilidad de los datos (de forma que la información sea utilizada por los usuarios autorizados).

Deber de secreto. El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los datos y al deber de guardarlos incluso después de finalizar sus relaciones con el titular del fichero automatizado.

l) ¿Cómo se puede acceder a los datos?

Acceso a los datos. Todo interesado puede solicitar y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, su origen y las comunicaciones realizadas o que se prevea realizar. Este derecho puede ejercerse únicamente en intervalos no inferiores a doce meses.

Con carácter previo puede ejercerse el derecho de consulta, que implica el derecho a conocer la existencia de un determinado tratamiento de datos de carácter personal pidiendo información al Registro General de Protección de Datos.

Rectificación y cancelación. Como consecuencia del ejercicio de los derechos de rectificación y cancelación que hemos expuesto anteriormente, el responsable del tratamiento tiene la obligación de hacer efectivo el derecho de rectificación o cancelación en el plazo de diez días. Cancelar no es sinónimo de borrar, sino que implica bloquear los datos conservándolos únicamente para que la Administración o los tribunales puedan determinar, si procede, las responsabilidades nacidas del tratamiento. La regulación del ejercicio de los derechos de rectificación y cancelación se encuentra en el Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999. Es interesante señalar que para aquellos casos en los que el ejercicio de tales derechos haya dado un resultado infructuoso por la oposición y reticencias del responsable del fichero o del encargado del tratamiento, la LOPD contempla un procedimiento de tutela ante la Agencia Española de Protección de Datos. Además, si se han causado daños o lesión en los bienes o derechos de los afectados tienen derecho a ser indemnizados.

m) ¿Qué es la transferencia internacional de datos?

En relación con el movimiento internacional de datos, hay que tener en cuenta que la Directiva 95/46 establece el sistema de protección de datos en base al principio según el cual los datos de carácter personal constituyen bienes que se integran dentro del comercio. En consecuencia, las libertades de tráfico

de bienes, personas y servicios que se establecen como libertades básicas para la consecución de la Unión Europea se aplican de forma idéntica a los datos como cualquier otro bien.

Por lo tanto, solo hay una transferencia internacional de datos cuando el país de destino es un estado no miembro de la Unión Europea. En relación con estos países, la LOPD establece que no pueden realizarse transferencias internacionales de datos a países que no proporcionen niveles de protección y seguridad equiparables a los previstos en la misma norma, salvo que lo autorice la Agencia Española de Protección de Datos. La Directiva 95/46 establece que la Comisión puede hacer constar que un tercer país garantiza un nivel de protección adecuado.

n) El análisis de riesgos y las medidas de tratamiento y seguridad

Los tratamientos deben ser objeto de un análisis de riesgos. Para ello pueden utilizarse las metodologías diseñadas al efecto[6]. Cuando los tratamientos puedan suponer un alto riesgo para los derechos y libertades de los interesados, deberán ser objeto de una evaluación de impacto sobre la protección de datos[7]. Sin embargo, si el tratamiento persigue una finalidad de interés público vinculado al ejercicio de poderes públicos, puede no llevarse a cabo la evaluación de impacto a pesar de tratarse de tratamientos de alto riesgo.

(6)Véase Agencia Española de Protección de Datos (2014). *Guía para una evaluación de impacto en la protección de datos*. Acceso en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

(7)El RGDP presume que, en determinados casos, existe un alto riesgo y dispone que las autoridades de control pueden publicar listas de tratamientos de alto riesgo.

En función de los riesgos, los responsables y encargados de tratamiento deben adoptar las medidas necesarias[8]. Estas medidas deben garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

(8)Véase al respecto lo previsto en el Esquema Nacional de Seguridad que debe interpretarse a la luz de lo dispuesto en el RGPD.

Las medidas se adoptarán tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento y para garantizar un nivel de seguridad adecuado al riesgo.

Asimismo, se deberán establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos, reaccionar ante ellas y notificar dichas violaciones a las autoridades de protección de datos y, en su caso, a los interesados.

o) Los responsables y los encargados del tratamiento

Las administraciones públicas, cuando sean responsables del tratamiento, deben aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD[9]. Estas medidas

(9)Artículo 24 RGPD.

deben ser acordes a 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.

Entre estas medidas se encuentra la de elegir un encargado de tratamiento al que el RGPD atribuye obligaciones específicas. El encargado debe ofrecer garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de acuerdo con las instrucciones del responsable, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado[10].

(10)Artículo 28 RGPD.

p) El delegado de protección de datos en una Administración pública

Cuando el tratamiento lo lleve a cabo una Administración pública, el responsable y el encargado del tratamiento deben designar un delegado de protección de datos[11]. Se puede designar un único delegado de protección de datos para varias administraciones públicas u organismos, teniendo en cuenta su estructura organizativa y tamaño.

(11)Artículo 37 RGPD. Véase Agencia Española de Protección de Datos (2017).*El Delegado de Protección de Datos en las Administraciones Públicas*. Acceso en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Funciones_DPD_en_AAPP.pdf

El delegado de protección de datos debe ser designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la regulación y la práctica en materia de protección de datos, así como a su capacidad para desempeñar las funciones previstas en el RGPD.

El delegado de protección de datos puede formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios. Además, el delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

El delegado de protección de datos tiene diversas funciones, entre las que destacan las siguientes[12]:

(12)Artículo 39 RGPD.

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El responsable y el encargado del tratamiento deben garantizar que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales y que no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. El delegado de protección de datos no puede ser destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones.

q) Los códigos de conducta, los mecanismos de certificación y las normas corporativas vinculantes (BCR)

El RGPD prevé que los responsables de tratamiento pueden adoptar diferentes instrumentos para acreditar el cumplimiento de las obligaciones previstas.

La adhesión a un código de conducta o a un mecanismo de certificación puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento[13].

(13)Articulo 24 RGPD.

Las administraciones públicas pueden adoptar códigos de conducta, así como promover la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del RGPD[14]. Los códigos de conducta deben recoger diferentes aspectos relativos a la aplicación del RGPD en relación con la administración pública que lo adopta, como la recogida de datos personales, la información que se facilita a los interesados, los derechos de los interesados, las responsabilidades del responsable y del encargado del tratamiento, las medidas de seguridad adoptadas o los mecanismos de resolución de conflictos y de control del cumplimiento del código[15].

(14)Articulo 40 RGPD.

(15)Artículo 40 RGPD.

Las administraciones públicas también pueden adoptar con carácter voluntario certificaciones, de sellos y marcas de protección de datos, para demostrar el cumplimiento de lo dispuesto en el RGPD en las operaciones de tratamiento de los responsables y los encargados que lleven a cabo[16]. Las administraciones públicas, junto con las autoridades de control, deben promover la creación de estos mecanismos de certificación en materia de protección de datos.

(16)Artículo 42 RGPD.

Finamente, las administraciones públicas pueden adoptar normas corporativas vinculantes (BCR) como garantía para poder realizar transferencias internacionales sin la necesidad de obtener una autorización específica cuando la Comisión no haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate, garantizan un nivel de protección adecuado. Las normas corporativas vinculantes serán aprobadas por la autoridad de control[17].

(17)Artículo 47 RGPD.

Cuando exista autorización por parte de la autoridad de control competente, las administraciones públicas pueden adoptar las garantías mediante disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

r) Qué pasa si se infringe la regulación de la protección de datos personales?

La LOPD establece un régimen específico para las infracciones cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza. En estos casos, se dispone que el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción[18]. Asimismo, se preveía la posibilidad de que el órgano sancionador pudiese proponer también la iniciación de actuaciones disciplinarias. Sin embargo, no se preveía la posibilidad de imponer las sanciones de multa previstas aplicables para los ficheros de titularidad privada y los tratamientos realizados por entidades privadas.

(18) Artículo 44 LOPD.

El RGPD abre la posibilidad de cambiar esta situación al prever que, más allá de los poderes correctivos de las autoridades de control, cada Estado miembro puede establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro[19].

(19) Artículo 83.7 RGPD.

2. Los datos personales en la Administración pública

Lectura propuesta

A. Cerrillo Martínez. *La administración electrónica y la protección de datos personales*. Módulo didáctico. UOC.

En relación con los distintos usos de los medios electrónicos en la Administración pública, se propone la lectura de los siguientes trabajos:

a) Difusión de la información del sector público

Estos trabajos abordan la tensión entre la transparencia y la difusión de información del sector público y la protección de los datos personales en poder de las administraciones públicas:

Cerrillo i Martínez, A. (2017). "El difícil equilibrio entre transparencia pública y la protección de datos personales". *Cuadernos de Derecho Local* (núm. 45).

Guichot Reina, E. (2017). "Las relaciones entre publicidad y privacidad en la normativa sobre transparencia y acceso a la información". *Cuadernos de Derecho Local* (núm. 44, pág. 12-47).

b) Tramitación del procedimiento administrativo

Estos trabajos analizan el impacto de la protección de los datos personales en la tramitación del procedimiento administrativo a través de medios electrónicos y el impacto de la interoperabilidad. También se debe que tener en cuenta la regulación de la firma electrónica y su uso en las relaciones entre las administraciones públicas y los ciudadanos.

Nota

Debe advertirse que estos trabajos son anteriores a la entrada en vigor de la Ley 39/2015 y 40/2015.

Troncoso Reigada, A. (2008). "La administración electrónica y la protección de datos personales". *Revista Jurídica de Castilla y León*. <http://www.navarra.es/NR/rdonlyres/E6188543-88F9-476F-8581-406069 D3C0E7/188896/32Administracionelectronicayprotecciondedatos Tronc.pdf>

Rallo Lombarte, A. (2010). "La Administración electrónica y el derecho a la protección de datos personales". En: C. de la Hera Pascual (ed.). *Administración electrónica: estudios, buenas prácticas y experiencias en el ámbito local*. Madrid: Fundación Democracia y Gobierno Local.
<http://repositorio.gobiernolocal.es/xmlui/bitstream/handle/10873/967/claves12_06_rallo.pdf?sequence=1>

Bibliografía

Fernández Salmerón, M.; Valero Torrijos, J. (2008). "La difusión de información administrativa en Internet y la protección de los datos personales: análisis jurídico de un proceso de armonización". En: A. Troncoso Reigada (ed.). *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos*. Madrid: Thomson-Civitas.

Guichot Reina, E. (2007). "Acceso a la información en poder de la Administración y protección de datos personales". *Revista de Administración Pública* (núm. 173).

Guichot Reina, E. (2007). "Derecho a la privacidad, transparencia y eficacia administrativa: un difícil y necesario equilibrio". *Revista Catalana de Dret Públic* (núm. 35).

Guichot Reina, E. (2008). "Acceso a la información y protección de datos. Estado de la cuestión". En: A. Troncoso Reigada (ed.). *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos*. Madrid: Thomson-Civitas.

Rallo Lombarte, A. (2010). "La Administración electrónica y el derecho a la protección de datos personales". En: C. de la Hera Pascual (ed.). *Administración electrónica: estudios, buenas prácticas y experiencias en el ámbito local*. Madrid: Fundación Democracia y Gobierno Local.

Troncoso Reigada, A. (2008). "La administración electrónica y la protección de datos personales". *Revista Jurídica de Castilla y León*.