La protección de datos personales en la administración pública

PID_00272672

Agustí Cerrillo Martínez

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Agustí Cerrillo Martínez

Catedrático de Derecho Administrativo en la Universitat Oberta de Catalunya (UOC).

La revisión de este recurso de aprendizaje UOC ha sido coordinada por el profesor: Agustí Cerrillo Martínez (2020)

Tercera edición: febrero 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

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

J. J. Fernández Rodríguez (2018). "Decálogo sobre a nova normativa de protección de datos". *Administración & cidadanía: Revista da Escola Galega de Administración Pública* (vol. 2, núm. 13, págs. 61-78). <https://egap.xunta.gal/Documentos/Publicacions/[1563537639]Revista_AC_13_2_web.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) ¿Qué impacto tiene la protección de datos en la transparencia pública?

Lecturas propuestas

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

E. Guichot Reina (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).

e) ¿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

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

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]

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 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), y, en determinados aspectos, mediante la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información (LSSI). La LOPDGDD derogó la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).

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. La Agencia de Protección de Datos de la Comunidad de Madrid fue suprimida el 1 de enero de 2013 por la Ley 8/2012, de 28 de diciembre, de medidas fiscales y administrativas 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. Al respecto, el RGPD reconoce que los códigos de conducta están destinados a contribuir a la correcta aplicación del Reglamento a través de la especificación de su aplicación en relación con aspectos como el tratamiento leal y transparente, los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos, la recogida de datos personales, la información proporcionada al público y a los interesados o el ejercicio de los derechos de los interesados. El código de conducta ha de contener mecanismos que permitan efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo. El código será registrado y publicado por la autoridad de control correspondiente.

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

La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal 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 reclamaciones de los afectados.

- Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento y de los responsables y encargados del tratamiento sobre las obligaciones que les afectan.

- Cooperar, en particular, compartiendo información con otras autoridades de control y prestar asistencia mutua a fin de garantizar la coherencia en la aplicación y ejecución del RGPD.

Para conseguir estos fines, el mismo reglamento reconoce toda una serie de potestades como las de ordenar al responsable y al encargado del tratamiento que faciliten cualquier información, llevar a cabo investigaciones en forma de auditorías de protección de datos, llevar a cabo una revisión de las certificaciones expedidas o notificar al responsable o encargado del tratamiento las presuntas infracciones del Reglamento.

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. En la actualidad, la Autoridad Catalana de Protección de Datos, creada por la Ley 32/2010, de 1 de octubre, dispone que tiene por objeto garantizar, en el ámbito de las competencias de la Generalitat, los derechos a la protección de datos personales y de acceso a la información que está vinculada a ella.

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.

g) ¿Qué es un dato personal?

La primera cuestión que hay que delimitar es la relativa a qué se entiende por *dato*. De acuerdo con el RGPD, un dato personal es cualquier información sobre una persona física identificada o identificable (el interesado). Se debe considerar persona física identificable cualquier persona cuya identidad se puede determinar, directa o indirectamente, mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de esta persona.

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.

El uso de las nuevas tecnologías ha planteado en el pasado si determinada información había de ser considerada como dato de carácter personal. En particular, la pregunta se había formulado respecto a si la dirección electrónica y la dirección IP eran 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".

h) ¿Cuáles son los principios relativos al tratamiento?

Los principios relativos al tratamiento son aquellas reglas que regulan cómo se tienen que llevar a cabo los tratamientos de datos personales con el fin de garantizar su la protección.

De este modo, los datos personales tienen que ser necesariamente tratados de acuerdo con los principios previstos en el RGPD. La vulneración de los principios previstos en el RGPD se tipifica en la normativa vigente como infracción muy grave.[5]

(5) Artículos 83 RGPD y 72 LOPDGDD.

El RGPD ha llevado a cabo una actualización de los diferentes principios a los cuales haremos referencia a continuación. Sin embargo, en términos generales, la regulación de los principios del tratamiento tiene un carácter continuista respecto a la regulación anterior, a pesar de que se han incorporado nuevos principios como el de responsabilidad proactiva.

Principios de licitud, lealtad y transparencia. Los datos personales tienen que ser tratados de manera lícita, leal y transparente en relación con el interesado.[6]

(6) Artículo 5.1.a RGPD.

Para que el tratamiento sea lícito hace falta que se dé alguna de las condiciones previstas en el RGPD.[7]

(7) Artículo 6.1 RGPD.

La principal condición para que el tratamiento sea lícito es que el interesado haya dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. El consentimiento tiene que ser libre, específico, informado e inequívoco por el cual acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que lo conciernen.[8]

(8) Artículo 4.11 RGPD.

Para que el consentimiento pueda manifestarse adecuadamente, hay que facilitar a los interesados información sobre el tratamiento de manera concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.[9] El RGPD prevé que la información que se tenga que facilitar al interesado será diferente cuando los datos personales se obtengan del interesado (artículo

(9) Artículo 12 RGPD.

(10) Artículo 11 LOPDGDD.

13.1) respecto a cuándo los datos personales no se hayan obtenido del interesado (artículo 14.1 y 2). En ambos casos, el responsable del tratamiento puede facilitar al afectado la información básica indicándole la dirección de correo electrónico o el medio a su disposición para poder acceder a la restante información.[10]

Además de los supuestos en que el interesado ha dado su consentimiento, los tratamientos de datos personales pueden ser lícitos si son necesarios para la ejecución de un contrato en el cual el interesado sea parte o para la aplicación a petición de este de medidas precontractuales, para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, para proteger intereses vitales del interesado o de otra persona física, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, o para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre estos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales.[11]

(11)Artículo 6.1 RGPD.

Lectura propuesta

A. Cerrillo Martínez (2019, julio). "Las características del consentimiento del interesado y su incidencia en el tratamiento de datos en las administraciones públicas". *El Consultor de los Ayuntamientos*, III.

Principio de limitación de la finalidad. Los datos personales tienen que ser recogidos con finalidades determinadas, explícitas y legítimas, y no serán tratados ulteriormente de manera incompatible con estas finalidades.[12]

(12)Artículo 5.1.b RGPD.

En relación con la limitación de la finalidad, la LRJSP[13] prevé que si bien las administraciones públicas deben facilitar a otras administraciones públicas el acceso a los datos relativos a los interesados que obren en su poder, estas no pueden llevar a cabo un tratamiento de dichos datos con finalidades incompatibles con la finalidad para la que se recogieron inicialmente los datos personales.

(13)Artículo 155 apartados 2 y 3 LRJSP modificados por el Real decreto ley 14/2019 de 31 de octubre.

En particular, se establece que cuando la Administración pública cesionaria de los datos pretenda su tratamiento ulterior para una finalidad que estime compatible con la finalidad inicial, deberá comunicarlo previamente a la Administración pública cedente para que esta pueda comprobar dicha compatibilidad. Esta podrá oponerse de manera motivada en el plazo de diez días.

Hasta que la Administración pública cedente no comunique su decisión, la Administración pública cesionaria no podrá utilizar los datos para la nueva finalidad pretendida, excepto que así esté previsto en una norma con rango de ley.

Este precepto también dispone que el tratamiento posterior de los datos personales con fines de archivo en interés público, con fines de investigación científica e histórica o con fines estadísticos no se considera incompatible con las finalidades iniciales.[14]

(14)Véase al respecto lo que dispone el artículo 26 LOPDGDD.

Principio de minimización de datos. Los datos personales tienen que ser adecuados, pertinentes y limitados a lo que es necesario en relación con las finalidades para las cuales son tratados.[15]

(15)Artículo 5.1.c RGPD.

De este modo, hay que asegurar que únicamente se recogen los datos personales necesarios para conseguir la finalidad prevista.

Principio de exactitud. Los datos personales tienen que ser exactos y, si es preciso, actualizados.[16]

(16)Artículo 5.1.d RGPD.

Para ello, hay que adoptar todas las medidas razonables para que se supriman o rectifiquen sin más dilación los datos personales que sean inexactos respecto a los fines para los cuales se tratan.

Principio de seguridad. Los datos personales tienen que ser tratados de tal manera que se garantice de manera adecuada su seguridad para evitar, entre otros, el tratamiento no autorizado o ilícito, la pérdida, destrucción o daño accidental.

De este modo se persigue garantizar la integridad y la confidencialidad de los datos.

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

Para garantizar el cumplimiento de estos principios, el RGPD reconoce diferentes derechos de los interesados. El RGPD ha reforzado los derechos de los interesados en materia de protección de datos. También ha ampliado los derechos, entre los cuales podemos destacar el derecho al olvido que, con anterioridad a su regulación en el RGPD, fue objeto de atención por el Tribunal de Justicia de la Unión Europea.[17]

(17)Sentencia del TJUE, de 13 de mayo de 2014, asunto C - 131/12 Google Spain, S. L. y Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González.

(18)Título X LOPDGDD.

Junto con los derechos reconocidos en el RGPD, la LOPDGDD reconoce otros derechos de los ciudadanos en internet, como el derecho a la educación digital, el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, el derecho a la desconexión digital en el ámbito laboral, el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el puesto de trabajo, el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral o el derecho al olvido en búsquedas de internet.[18]

En relación con los diferentes derechos reconocidos, se debe tener presente los siguientes aspectos de carácter general.

En primer lugar, que el responsable del tratamiento está obligado a indicar al interesado los medios a su disposición para ejercer los derechos. Estos medios deben ser fácilmente accesibles.[19]

(19)Artículo 12 LOPDGDD.

En segundo lugar, que los derechos reconocidos en el RGPD pueden ser limitados cuando, con la restricción, se respeten los derechos y libertades fundamentales y sea una medida necesaria y proporcionada para salvaguardar, entre otros, la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, la protección de la independencia judicial, la supervisión, inspección o reglamentación vinculada con el ejercicio de la autoridad pública o la protección del interesado o de los derechos y libertades de otros.[20]

(20)Artículo 23 RGPD.

En tercer lugar, que en el supuesto de que no se respeten los derechos reconocidos en el RGPD, el interesado puede presentar una reclamación ante la Agencia Española de Protección de Datos o agencia autonómica de protección de datos competente que tenga que resolver sobre la cuestión.[21] Asimismo, el impedimento o la obstaculización del ejercicio de los interesados están tipificados como infracción.[22]

(21)Considerando 141 RGPD, así como, entre otros, los artículos 12.4, 13.2, 14.2, 15.1 RGPD.

(22)Artículos 83 RGPD y 72.1.ky 74.cyd LOPDGDD.

Derecho de información. La transparencia en el tratamiento de los datos personales se concreta en el derecho a la información de los interesados.

Como ya hemos avanzado anteriormente, los responsables del tratamiento tienen que informar al interesado de varios aspectos que variarán en función de si los datos han sido recogidos del interesado o no.

Sin embargo, el RGPD dispone algunas excepciones a este derecho como, por ejemplo, cuando la información ya esté a disposición del interesado.[23]

(23)Artículo 14.5 RGPD.

En términos generales, la información se debe poner a disposición de los interesados en el momento en que se le soliciten sus datos, o cuando los datos no se obtengan del propio interesado, en el plazo de un mes.[24]

(24)Artículo 14.3 RGPD.

Derecho de acceso. El interesado tiene derecho a saber si se están tratando o no sus datos personales.[25]

(25)Artículo 15.1 RGPD.

El interesado también tiene derecho a acceder a estos datos y a obtener la información relativa a diferentes aspectos como los fines del tratamiento; las categorías de datos personales de que se trate; los destinatarios o las categorías de destinatarios a los cuales se comunicaron o serán comunicados los datos personales; el plazo previsto de conservación de los datos personales o, si no es posible, los criterios utilizados para determinar este plazo; la existencia del derecho a solicitar al responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado o la oposición a este tratamiento; el derecho a presentar una reclamación ante una autoridad de control o la información disponible sobre su origen cuando los datos personales no se hayan obtenido del interesado, y la existencia de decisiones automatizadas.

Cuando así lo solicite el interesado, el responsable del tratamiento le facilitará una copia de los datos personales objeto de tratamiento sin que esto pueda afectar negativamente a los derechos y libertades de terceros. La LOPDGDD dispone que el derecho se entenderá otorgado si el responsable del tratamiento facilita al interesado un sistema de acceso remoto, directo y seguro a sus datos personales.[26]

(26)Artículo 13 RGPD.

Derecho de rectificación. El interesado tiene derecho a obtener sin más dilación indebida la rectificación de los datos personales inexactos que le conciernan.[27]

(27)Artículo 16 RGPD.

El interesado tiene derecho a que se completen los datos personales que sean incompletos.

A estos efectos, el interesado debe indicar de manera clara y detallada a qué datos se refiere y la corrección que se tenga que hacer y, cuando sea preciso, acompañar la solicitud de la documentación que justifique la rectificación.[28]

(28)Artículo 14 LOPDGDD.

Derecho de supresión. El interesado tiene derecho a obtener sin más dilación indebida la supresión de los datos personales que le conciernan.[29]

(29)Artículo 17 RGPD.

El responsable del tratamiento estará obligado a suprimir los datos personales del interesado cuando estos ya no sean necesarios en relación con las finalidades para las cuales fueron recogidos o tratados de otro modo, el interesado retire el consentimiento en que se basa el tratamiento, el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento, los datos personales hayan sido tratados ilícitamente, los datos personales se deban suprimir para el cumplimiento de una obligación legal o se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

El derecho de supresión puede ser limitado cuando el tratamiento sea necesario para ejercer el derecho a la libertad de expresión e información; para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; por razones de interés público en el ámbito de la salud pública; con fines de archivo en interés público, de investigación científica o histórica o finalidades estadísticas o para la formulación, el ejercicio o la defensa de reclamaciones.

Derecho a la limitación del tratamiento. El interesado tiene derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos.

La limitación del tratamiento se podrá obtener cuando el interesado haya impugnado la exactitud de los datos personales; o el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; o el responsable ya no necesite los datos personales para las finalidades del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; o el interesado se haya opuesto al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.[30]

(30)Artículo 18 RGPD.

Cuando se haya limitado el tratamiento de datos personales, los datos solo pueden ser objeto de tratamiento, a excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o en orden a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante.

Derecho de oposición. El interesado tiene derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, al hecho de que datos personales que le conciernen sean objeto de un tratamiento.[31]

(31)Artículo 21 RGPD.

En este caso, el responsable del tratamiento debe dejar de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Una manifestación concreta de este derecho la encontramos en el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de los datos personales que produzca efectos jurídicos en él o le afecte significativamente de manera similar.[32]

(32)Artículo 22 RGPD.

j) 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.[33] Estas medidas 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.

(33)Artículo 24 RGPD.

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.[34]

(34)Artículo 28 RGPD.

k) 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.[35] Se puede designar un único delegado de protección de datos para varias administraciones públicas u organismos, teniendo en cuenta su estructura organizativa y tamaño.

(35)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:[36]

(36)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.

l) 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.[37]

(37)Artículo 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.[38] 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.[39]

(38)Artículo 40 RGPD.

(39)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

(40)Artículo 42 RGPD.

de los responsables y los encargados que lleven a cabo.[40] Las administraciones públicas, junto con las autoridades de control, deben promover la creación de estos mecanismos de certificación en materia de protección de datos.

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.[41]

(41)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.

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

La LOPD establecía un régimen específico para las infracciones cometidas en ficheros de titularidad pública o en relación con tratamientos los responsables lo eran de ficheros de esta naturaleza. En estos casos, se disponía que el órgano sancionador dictaría una resolución para establecer las medidas que procediera adoptar para que cesaran o se corrigieran los efectos de la infracción. Asimismo, se preveía la posibilidad de que el órgano sancionador pudiera 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.

El RGPD abrió 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 el mencionado Estado miembro.

Esta posibilidad ha sido prácticamente cerrada por la LOPDGDD.

Esta norma dispone de un régimen sancionador aplicable a determinadas categorías de responsables o encargados del tratamiento, entre las que se encuentran las siguientes:

- Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
- Los órganos jurisdiccionales.
- La Administración General del Estado, las administraciones de las comunidades autónomas y las entidades que integran la Administración local.
- Los organismos públicos y entidades de derecho público vinculadas o dependientes de las administraciones públicas.
- Las autoridades administrativas independientes.
- El Banco de España.
- Las corporaciones de derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
- Las fundaciones del sector público.
- Las universidades públicas.
- Los consorcios.
- Los grupos parlamentarios de las Cortes Generales y las asambleas legislativas autonómicas, así como los grupos políticos de las corporaciones locales.

Cuando un responsable o encargado incluido entre estas categorías cometa una infracción, la autoridad de protección de datos que resulte competente dictará resolución sancionándolos con apercibimiento. Asimismo, se concretarán las medidas que se deben adoptar para que cese la conducta o se corrijan los efectos de la infracción que se haya cometido. Además, si las infracciones son imputables a autoridades y directivos y se acredita la existencia de informes técnicos o recomendaciones para el tratamiento que no hayan estado debidamente atendidos, en la resolución en la cual se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará su publicación en el Boletín Oficial del Estado o autonómico que corresponda.

La LOPDGDD también dispone que la resolución se notificará al responsable o encargado del tratamiento, al órgano del cual dependa jerárquicamente y a los afectados que tengan la condición de interesados. Además, las resoluciones se publicarán en la página web de la Agencia Española de Protección de

Datos cuando esta sea la autoridad competente, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Asimismo, se prevé que la autoridad de protección de datos proponga la iniciación de actuaciones disciplinarias cuando haya indicios suficientes de acuerdo con lo que prevé la legislación sobre régimen disciplinario o sancionador que sea aplicable. Las resoluciones al respecto se tendrán que comunicar a la autoridad de protección de datos.

Finalmente, la LOPDGDD dispone que se deben comunicar al Defensor del Pueblo o, si procede, a las instituciones análogas de las comunidades autónomas, las actuaciones realizadas y las resoluciones dictadas.

Bibliografía

Agencia Española de Protección de Datos (2018). *Protección de datos y administración local*. Madrid: Agencia Española de Protección de Datos.

Grupo de trabajo para la implantación del nuevo Reglamento General de Protección de Datos (RGPD) en las Administraciones Locales-Federación Española de Municipios y Provincias (2018). *Guía para la adaptación del Reglamento General de Protección de Datos de las Administraciones Locales*. Madrid: Federación Española de Municipios y Provincias.

Jiménez Asensio, R. (2019). "El nuevo marco normativo de la protección de datos personales: su aplicación a las entidades locales". *Anuario Aragonés del Gobierno Local 2018* (núm. 10, págs. 321-365).

Jiménez Asensio, R.; Moro, A. (2018). *Manual-guía sobre impactos del Reglamento (UE) de protección de datos en los entes locales*. Barcelona: Federació de Municipis de Catalunya-Associació Catalana de Municipis.