

---

# La administración electrónica y la protección de datos personales

---

PID\_00248571

Agustí Cerrillo Martínez

---

Tiempo mínimo de dedicación recomendado: 4 horas





Los textos e imágenes publicados en esta obra están sujetos –excepto que se indique lo contrario– a una licencia de Reconocimiento-NoComercial-SinObraDerivada (BY-NC-ND) v.3.0 España de Creative Commons. Podéis copiarlos, distribuirlos y transmitirlos públicamente siempre que citéis el autor y la fuente (FUOC. Fundació para la Universitat Oberta de Catalunya), no hagáis de ellos un uso comercial y ni obra derivada. La licencia completa se puede consultar en <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.es>

# Índice

<b>Introducción.....</b>	<b>5</b>
<b>Objetivos.....</b>	<b>6</b>
<b>1. La administración electrónica y su impacto en la protección de los datos personales.....</b>	<b>7</b>
<b>2. Los fundamentos jurídicos de la administración electrónica</b>	<b>10</b>
2.1. La regulación de la administración electrónica .....	10
2.2. Los principios generales de la administración electrónica. La seguridad en la administración electrónica .....	12
2.3. Los derechos y las obligaciones en la administración electrónica .....	14
2.4. El acceso a la información y los servicios a través de medios electrónicos .....	16
<b>3. El procedimiento administrativo electrónico.....</b>	<b>18</b>
3.1. La identificación y la firma electrónicas .....	18
3.1.1. La identificación y la firma electrónicas de los interesados .....	18
3.1.2. La identificación y la firma electrónicas de las Administraciones públicas .....	20
3.2. La iniciación del procedimiento .....	20
3.3. La ordenación del procedimiento administrativo .....	21
3.4. La instrucción del procedimiento .....	22
3.5. La finalización del procedimiento .....	23
<b>4. Las especialidades del tratamiento de datos personales en las Administraciones públicas.....</b>	<b>25</b>
4.1. La creación de ficheros en las Administraciones públicas .....	25
4.2. Las obligaciones de los responsables del tratamiento. Las relaciones entre los responsables del tratamiento y los encargados del tratamiento .....	26
4.3. La adhesión a los códigos de conducta, mecanismos de certificación, normas corporativas vinculantes (BCR) .....	27
4.4. La designación y posición del delegado de protección de datos en una Administración pública .....	28
4.5. Régimen sancionador aplicable a las Administraciones públicas .....	29
<b>5. El gobierno abierto y la protección de datos personales.....</b>	<b>31</b>

5.1. La difusión de información pública .....	32
5.2. El acceso a la información pública .....	33
5.3. La reutilización de información pública .....	35
5.4. La protección de datos personales como límite a la transparencia pública .....	38
<b>6. Las relaciones interadministrativas por medios electrónicos. Las comunicaciones de datos entre Administraciones públicas.....</b>	<b>42</b>
6.1. La cooperación interadministrativa por medios electrónicos .....	42
6.2. Las comunicaciones de datos entre Administraciones públicas .....	44
<b>Abreviaturas.....</b>	<b>49</b>
<b>Bibliografía.....</b>	<b>50</b>

## Introducción

Las Administraciones públicas, en el desarrollo de sus funciones, recaban ingentes cantidades de datos personales de la ciudadanía. El uso de los medios electrónicos en el desarrollo de las actividades de las Administraciones públicas y en sus relaciones con la ciudadanía puede poner en riesgo dichos datos personales. Para hacer frente a las posibles amenazas y riesgos, cuando las Administraciones públicas y la ciudadanía utilizan los medios electrónicos, debe valorarse la existencia de datos personales y, en su caso, adoptar las medidas previstas respecto a su tratamiento adecuado y seguridad. Como pone de manifiesto el documento elaborado por el Grupo de Trabajo sobre Protección de Datos del Artículo 29, el éxito de algunos de los proyectos de administración digital depende de complejas cuestiones relacionadas con la protección de datos a los que se debe prestar la atención adecuada (Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2003).

Asimismo, en el marco de los proyectos de gobierno abierto que están impulsando en la actualidad las Administraciones públicas, estas tienen el desafío de conseguir la apertura de los datos públicos para facilitar la toma de decisiones y la reutilización, sin que ello afecte a la protección de los datos personales. Como señala la Comisión Europea, «los objetivos de promover los datos abiertos de la Administración pública y proteger los datos personales pueden reforzarse mutuamente si se basan en una gestión proactiva y consciente de la información por parte del sector público» (Comisión Europea, 2011, pág. 6).

A lo largo de este módulo se analizan los fundamentos de la administración electrónica y se identifican los aspectos vinculados a la protección de los datos personales que deben tenerse en cuenta cuando las Administraciones públicas utilizan los medios electrónicos en sus relaciones con la ciudadanía en la tramitación del procedimiento administrativo. Asimismo, se exponen las especificidades que prevé la normativa vigente en relación con el tratamiento de datos personales en las Administraciones públicas. Además, también se muestra el impacto que la protección de datos personales tiene en el impulso del gobierno abierto. Finalmente, se muestra cómo el régimen relativo a la cesión de datos incide en las relaciones entre Administraciones públicas a través de medios electrónicos.

## Objetivos

- 1.** Conocer los fundamentos del uso de los medios electrónicos en el funcionamiento de las Administraciones públicas y en las relaciones entre las Administraciones públicas y la ciudadanía.
- 2.** Identificar las consecuencias de la administración electrónica en las relaciones entre los ciudadanos y las Administraciones públicas en relación con la protección de datos personales.
- 3.** Analizar las especificidades de la regulación del tratamiento de datos personales en las Administraciones públicas.
- 4.** Valorar el impacto de la protección de datos personales en el desarrollo de la administración electrónica y del gobierno abierto.

## 1. La administración electrónica y su impacto en la protección de los datos personales

La expresión *administración electrónica* comprende los diversos usos de los medios electrónicos en las Administraciones públicas y en sus relaciones con la ciudadanía. La administración electrónica consiste en el uso intensivo de los medios electrónicos por la Administración pública con el objetivo de mejorar la eficiencia interna, las relaciones interadministrativas y las relaciones de la Administración con los ciudadanos.

La administración electrónica persigue incrementar la eficacia de las Administraciones públicas al tiempo que se fortalece su apertura y transparencia y, en última instancia, se facilita la relación con la ciudadanía y la personalización de los servicios que les ofrecen. Algunos autores consideran que hoy en día no se debe hablar de administración electrónica sino de administración digital, lo que supone superar la automatización de los procesos de las Administraciones públicas en el que se centra la administración electrónica para repensar el funcionamiento de las Administraciones públicas a través de la innovación que se puede derivar del uso de los medios electrónicos y de la apertura de las Administraciones públicas<sup>1</sup>.

<sup>(1)</sup>Véase al respecto el 2016 Trends to watch (<https://goo.gl/XOhhwK>). En general, Cerrillo Martínez, 2016.

La administración electrónica tiene un carácter poliédrico, ya que presenta diferentes planos (técnicos, político-organizativo, jurídico) cuya intersección es necesaria para su óptimo desarrollo. En efecto, a pesar de que generalmente se relaciona la administración electrónica con el uso de la tecnología por las Administraciones públicas, el desarrollo de la administración electrónica tiene un alcance más amplio en la medida en que exige cambios organizativos y procedimentales que deben ser impulsados por un liderazgo político y técnico claro y decidido que determina el alcance del uso de la tecnología. Además, para avanzar en el desarrollo de la administración electrónica, es necesaria la regulación del uso y del impacto de los medios electrónicos en las Administraciones públicas que garantice tanto los derechos de los ciudadanos en sus relaciones con las Administraciones públicas a través de medios electrónicos como la seguridad jurídica de las transacciones electrónicas que se lleven a cabo a través de estos medios. De hecho, como manifiesta la conocida expresión de la OCDE, «la tecnología es un facilitador, pero no una solución», en efecto, la administración electrónica no es un asunto meramente técnico, sino de gobernanza democrática. Por ello, los efectos de los medios electrónicos solo se conseguirán en la medida que también se introduzcan cambios en las estructuras, en los procesos y en la manera como trabajan y se organizan los poderes públicos<sup>2</sup>. En esta dirección se manifestó la Comisión de la Unión Europea en su comunicación sobre «El papel de la administración electrónica en el futuro de Europa» [COM (2003) 567 final] afirmando que «el énfasis no

<sup>(2)</sup>Recomendación (2004) 15 del Comité de Ministros del Consejo de Europa.

debe ponerse en las TIC propiamente dichas, sino en su utilización *combinada* con los cambios organizativos y con nuevas aptitudes encaminadas a mejorar los servicios públicos, los procesos democráticos y las políticas públicas».

En los últimos años, las Administraciones públicas han hecho importantes esfuerzos para impulsar el uso de los medios electrónicos tanto en su actividad interna como en sus relaciones con la ciudadanía para, de esta manera, poder aprovechar todo el potencial que se deriva del uso de la tecnología. Este impulso ha venido concretado en la adopción de diversas estrategias que han definido los objetivos y acciones a impulsar.

Sin entrar en detalles, para conocer la tendencia que adoptará el desarrollo de la administración electrónica en los próximos años, puede resultar de utilidad traer a colación el Plan de Acción sobre Administración Electrónica de la Unión Europea para el periodo 2016-2020. Acelerar la transformación digital de la administración<sup>3</sup>, en el que se prevé lo siguiente:

<sup>(3)</sup>COM(2016) 179 final.

«En 2020, las Administraciones públicas y las instituciones públicas de la Unión Europea deben ser abiertas, eficaces e integradoras, proporcionando servicios públicos digitales a todos los ciudadanos y empresas de la UE que sean personalizados, transfronterizos, servicios fáciles de usar, y de extremo a extremo. Se usan enfoques innovadores para diseñar y ofrecer mejores servicios adecuados a las necesidades y demandas de los ciudadanos y las empresas. Las Administraciones públicas utilizan las oportunidades que ofrece el nuevo entorno digital para facilitar su interacción con las partes interesadas y entre ellas».

El Plan de Acción dispone que cualquier proyecto de administración electrónica que se impulse debe basarse en los siguientes principios: versión digital por defecto, principio de «una sola vez», inclusión y accesibilidad, apertura y transparencia, escala transfronteriza por defecto, interoperabilidad de forma predeterminada y fiabilidad y seguridad. Precisamente, el último principio es una muestra de la relación que el desarrollo de la administración electrónica tiene con la protección de datos personales. En efecto, como destaca la Comisión Europea, «todas las iniciativas deberían ir más allá del mero cumplimiento del marco jurídico sobre la protección de datos personales y de la intimidad y la seguridad informática, integrando estos elementos en la fase de diseño».

Los datos adquieren un papel muy significativo en la administración electrónica. En el ejercicio de sus funciones, las Administraciones públicas generan una multitud ingente de datos que deben gestionarse adecuadamente y que son muy útiles para la toma de decisiones. Asimismo, la ciudadanía y las empresas facilitan muchos datos a las Administraciones públicas tanto directa como indirectamente que son recabados en el ejercicio de sus funciones y que tienen un importante valor en la toma de decisiones y para la reutilización. Además, todos estos datos pueden ser objeto de análisis a través de la minería de datos y las técnicas de *big data*, lo que permite anticipar modelos de comportamiento de la ciudadanía, prestar servicios de manera proactiva o perso-



nalizar las actuaciones de las Administraciones públicas a las circunstancias de cada interesado, aproximando las expectativas a la prestación efectiva de los servicios.

El uso de datos personales en el desarrollo de las actividades de las Administraciones públicas y en sus relaciones con la ciudadanía puede poner en riesgo dichos datos, lo que exige adoptar las medidas organizativas, técnicas y jurídicas necesarias para evitarlos.

## 2. Los fundamentos jurídicos de la administración electrónica

### 2.1. La regulación de la administración electrónica

La regulación de la administración electrónica ha experimentado una evolución muy importante en los últimos años.

En 1992, España fue pionera en la regulación de los medios electrónicos en la actividad de las Administraciones públicas. La Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común reconocía que «las técnicas burocráticas formalistas, supuestamente garantistas, han caducado, por más que a algunos les parezcan inamovibles, y la Ley se abre decididamente a la tecnificación y modernización de la actuación administrativa en su vertiente de producción jurídica y a la adaptación permanente al ritmo de las innovaciones tecnológicas». Para ello, disponía en su artículo 45 que «las Administraciones públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias» y que «cuando sea compatible con los medios técnicos de que dispongan las Administraciones públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos o telemáticos». Posteriormente, en 2001, se añadieron dos disposiciones para facilitar el uso de los medios electrónicos en los registros administrativos (art. 38.9) y las notificaciones administrativas (art. 59.3).

En 2007, se aprobó la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Esta norma significó un cambio importante en la regulación del uso de los medios electrónicos. En efecto, como reconocía su exposición de motivos, «el desarrollo de la administración electrónica es todavía insuficiente. La causa en buena medida se debe a que las previsiones de los artículos 38, 45 y 59 de la Ley de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común son facultativas. Es decir, dejan en manos de las propias Administraciones determinar si los ciudadanos van a poder de modo efectivo, o no, relacionarse por medios electrónicos con ellas, según que estas quieran poner en pie los instrumentos necesarios para esa comunicación con la Administración. Por ello esta Ley pretende dar el paso del “podrán” por el “deberán”». En particular, la citada ley reguló el derecho a comunicarse con las Administraciones por medios electrónicos, así como el régimen jurídico de la administración electrónica. Además, de esta norma de forma paralela se fueron aprobando otras normas que incidían en la materia como la Ley 17/2009, de 23 de noviembre, sobre libre acceso a las actividades de servicios y su ejercicio, la Ley 2/2011,

de 4 de marzo, de economía sostenible, o la Ley 20/1013, de 9 de diciembre, de garantía de la unidad de mercado. Asimismo, debe tenerse presente la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y las normas autonómicas en la materia.

A pesar del impacto positivo de la Ley 11/2007, de 22 de junio en el desarrollo de la administración electrónica, no se puede desconocer que ha habido un incumplimiento generalizado de dicha norma, entre otros motivos por las dificultades de las administraciones públicas para poder disponer de los recursos necesarios para poder desplegar su contenido y la falta de herramientas adecuadas para imponer su cumplimiento. Asimismo, como señala Valero:

«La efectiva aplicación de las previsiones de la LAECSP se ha encontrado en la práctica con otras barreras que, en última instancia, nada tienen que ver con la existencia de dificultades presupuestarias. Antes al contrario, en gran medida se deben a la inexistencia de una voluntad clara de impulsar la modernización tecnológica de la respectiva entidad, proceso que en modo alguno está exento de dificultades que, en última instancia, podrían verse solventadas si existiese un proyecto institucional serio y con el oportuno liderazgo y respaldo al máximo nivel» (Valero Torrijos, 2012).

En 2015, el legislador, consciente de la dispersión normativa en materia de administración digital, trata de unificar la regulación del uso de los medios electrónicos por las Administraciones públicas a través de la aprobación de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones públicas y la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público. Según la exposición de motivos de la primera:

«La regulación de esta materia venía adoleciendo de un problema de dispersión normativa y superposición de distintos regímenes jurídicos no siempre coherentes entre sí, de lo que es muestra la sucesiva aprobación de normas con incidencia en la materia [...]

Ante este escenario legislativo, resulta clave contar con una nueva Ley que sistematice toda la regulación relativa al procedimiento administrativo, que clarifique e integre el contenido de las citadas Ley 30/1992, de 26 de noviembre y Ley 11/2007, de 22 de junio, y profundice en la agilización de los procedimientos con un pleno funcionamiento electrónico.»

Además de las normas a las que se ha hecho referencia aprobadas en España, también deben tenerse presente otras normas que son de aplicación por las Administraciones públicas españolas y que tienen un impacto específico en la administración electrónica como, por ejemplo, el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, que ha derogado la Directiva 1999/93/CE, 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, o la Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.

Asimismo, no puede desconocerse que en ocasiones la administración electrónica se ve regulada por decisiones adoptadas por los propios usuarios de la administración electrónica que bien informan sobre el concreto alcance de las normas vigentes en relación con un determinado proyecto de administración electrónica (por ejemplo, a través de un aviso legal), bien se comprometen al cumplimiento de determinados estándares (por ejemplo, adoptando un código de conducta).

## **2.2. Los principios generales de la administración electrónica. La seguridad en la administración electrónica**

La administración electrónica debe basarse en el respeto de diversos principios que definen el marco en el que debe desarrollarse cualquier proyecto de administración digital. Estos principios orientan el diseño y desarrollo de la administración digital y tienen una función interpretativa de la normativa reguladora de la administración electrónica colmando las lagunas que puedan surgir en su aplicación.

En la actualidad, la LRJSP recoge diferentes principios que inciden en el diseño y el desarrollo de la administración electrónica. Sin embargo, su alcance es diverso. Algunos de los principios tienen carácter general en relación con el conjunto de la actividad y las relaciones de las Administraciones públicas, mientras que otros únicamente se prevén en relación con la sede electrónica<sup>4</sup>.

<sup>(4)</sup>A diferencia de la LRJSP, la Ley 11/2007, de 22 de junio, hacía una regulación exhaustiva de los principios de la administración electrónica.

**1) Principio de igualdad:** todas las personas, independientemente de que utilicen medios electrónicos o no en sus relaciones con las Administraciones públicas, deben situarse en posición de igualdad y, por lo tanto, se debe evitar cualquier restricción o discriminación por razón del canal utilizado para ello. Este principio tiene una especial manifestación en relación con aquellos colectivos que pueden tener dificultades para acceder o utilizar los medios electrónicos.

**2) Principio de simplificación:** los medios electrónicos deben favorecer la eficacia administrativa a través de la reducción de los tiempos y plazos necesarios para la tramitación de los procedimientos administrativos, la disminución de las cargas documentales o la supresión o reducción de los trámites administrativos. Para ello, las administraciones deben acompañar el proceso de tecnificación con un rediseño funcional y de racionalización administrativa.

**3) Principio de transparencia:** los medios electrónicos deben facilitar el conocimiento de la actividad administrativa por parte de la ciudadanía. Asimismo, la ciudadanía debe tener conocimiento de la existencia y el alcance del uso de los medios electrónicos por parte de las Administraciones públicas, por ejemplo, a través de la adopción de cartas de servicios, la elaboración de guías

o catálogos de procedimientos y servicios que se pueden tramitar electrónicamente o la publicación de las características de los programas y aplicaciones que se utilicen.

**4) Principio de calidad:** las Administraciones públicas deben garantizar que, en diseño e implementación de los proyectos de administración electrónica, se garantizan las finalidades perseguidas. Para ello, deben impulsarse los avisos legales o las cartas de servicios que fijen los compromisos de calidad con los que se prestan los servicios públicos a través de los medios electrónicos.

**5) Principio de accesibilidad y usabilidad:** las Administraciones públicas deben garantizar que cualquier persona, independientemente de sus circunstancias personales, puede acceder a la información y a los servicios que se facilitan a través de medios electrónicos. Asimismo, deben facilitar que los proyectos de administración electrónica puedan ser utilizados por los usuarios de la manera más sencilla, efectiva y satisfactoria.

**6) Principio de cooperación e interoperabilidad:** las Administraciones públicas deben utilizar los medios electrónicos para intercambiar datos y, en la medida de lo posible, fomentar la prestación conjunta de servicios a la ciudadanía. Para ello, deben garantizar la interoperabilidad, es decir, la capacidad de los sistemas de información de compartir datos e intercambiar información.

**7) Principio de neutralidad:** las Administraciones públicas deben evitar que las opciones tecnológicas que tomen tanto ellas como la ciudadanía puedan condicionar negativamente el alcance de sus relaciones a través de medios electrónicos. La neutralidad exige que las Administraciones públicas no dependan de una determinada empresa o consultora que diseñe o desarrolle sus aplicaciones de administración electrónica.

**8) Principio de seguridad:** las Administraciones públicas deben adoptar las medidas necesarias para garantizar que el uso de los medios electrónicos no plantea problemas en relación con la integridad, la disponibilidad o la confidencialidad de los datos. Las medidas que se adopten deben ser proporcionales a las finalidades previstas.

En particular, para garantizar la seguridad de los datos, las aplicaciones deben contar con las medidas de seguridad previstas en el Esquema Nacional de Seguridad (ENS). La finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos a través de medidas que han de garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de forma que permita a los ciudadanos y a las Administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Entre los principios básicos del ENS que deben regir

toda acción orientada a asegurar la información y los servicios se encuentra la seguridad como proceso integral, la gestión basada en riesgos y el carácter diferenciado de la seguridad respecto a la gestión de la información.

Para la consecución de los objetivos del ENS se prevé que las Administraciones públicas deben adoptar un Plan de Adecuación<sup>5</sup>. Para su cumplimentación resulta de utilidad consultar las guías de implantación elaboradas por el Centro Criptológico Nacional<sup>6</sup>. Asimismo, las Administraciones públicas deben elaborar diferentes documentos que permiten hacer un seguimiento del cumplimiento de los diferentes requerimientos del ENS (declaración de aplicabilidad, declaración de conformidad, etc.) que deberán ser publicados en la sede electrónica<sup>7</sup>. Las Administraciones públicas también deberán someter a las auditorías periódicas sus sistemas de información de categoría media y alta.

<sup>(5)</sup>Véase al respecto: <https://goo.gl/8ONiQl>.

<sup>(6)</sup>Véase al respecto: <https://goo.gl/u6DKKl>.

<sup>(7)</sup>Anexo I Real decreto 3/2010, de 8 de enero.

Finalmente, es importante señalar la necesidad de identificar claramente a los responsables de velar por el cumplimiento de las medidas de seguridad que adopte cada Administración pública.

### 2.3. Los derechos y las obligaciones en la administración electrónica

La LPACAP reconoce diversos derechos de las personas y de los interesados que conforman el estatuto jurídico de las personas frente a las Administraciones públicas. Todos estos derechos son auténticos derechos subjetivos.

Con carácter general, la LPACAP reconoce el derecho de relacionarse electrónicamente con las Administraciones públicas. Este derecho se concreta en los siguientes derechos que tienen carácter complementario:

- derecho a elegir en todo momento si se comunican con las Administraciones públicas a través de medios electrónicos;
- derecho a comunicarse con las Administraciones públicas a través de un punto de acceso general electrónico de la Administración;
- derecho a ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones públicas especialmente en lo referente a la identificación y la firma electrónica, la presentación de solicitudes a través del registro electrónico general y la obtención de copias auténticas. Este derecho se canalizará a través de las oficinas de asistencia en materia de registros;
- derecho a la obtención y utilización de los medios de identificación y firma electrónica;

#### Derechos de las personas con las Administraciones públicas

La legislación autonómica ha ampliado el elenco de derechos de las personas en sus relaciones con las Administraciones públicas (Cerrillo Martínez, 2010b). Igualmente, algunas ordenanzas locales. Véase al respecto, la ordenanza tipo elaborada por la FEMP o por LOCALRET.

- derecho a la protección de datos de carácter personal;
- derecho a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones públicas.

Sin embargo, determinados sujetos no gozan de estos derechos y están obligados a comunicarse con las Administraciones públicas a través de medios electrónicos. En particular, los siguientes sujetos están obligados a utilizar los medios electrónicos para la realización de cualquier trámite de un procedimiento administrativo:

- personas jurídicas;
- entidades sin personalidad jurídica;
- quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones públicas en ejercicio de dicha actividad profesional;
- quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración;
- empleados públicos para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público, en la forma en que se determine reglamentariamente por cada Administración pública.

Asimismo, cada Administración pública podrá establecer reglamentariamente la obligación de relacionarse con ella a través de medios electrónicos para determinados procedimientos, para la presentación de escritos en el registro o para la recepción de notificaciones administrativas, y para ciertos colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos, quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

Los interesados, que son aquellos sujetos que intervienen en un procedimiento administrativo de acuerdo con lo previsto en la LPACAP, también tienen reconocidos los siguientes derechos relacionados con el uso de los medios electrónicos:

- derecho a conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados;
- derecho a acceder y a obtener copia de los documentos contenidos en los procedimientos administrativos;
- derecho a no presentar documentos originales salvo que, de manera excepcional, la normativa reguladora aplicable establezca lo contrario. En

caso de que se deba presentar un documento original, el interesado tendrá derecho a obtener una copia autenticada;

- derecho a no presentar datos y documentos que ya se encuentren en poder de las Administraciones públicas o que hayan sido elaborados por estas;
- derecho a cumplir las obligaciones de pago a través de medios electrónicos (por ejemplo, tarjeta de crédito y débito, transferencia bancaria o domiciliación bancaria).

La LPACAP no dispone de mecanismos de garantía de estos derechos como sí hacía la Ley 11/2007, de 22 de junio, al prever la figura del defensor del usuario de la administración electrónica en la Administración General del Estado<sup>8</sup>.

<sup>(8)</sup>En el tiempo en que la Ley 11/2007, de 22 de junio, estuvo en vigor no se llegó a poner en funcionamiento esta figura.

Finalmente, es de interés poner de relieve que, para que las personas y los interesados puedan ejercer sus derechos y cumplir con las obligaciones previstas en relación con el uso de los medios electrónicos, es necesario que las Administraciones públicas hayan desarrollado las aplicaciones y los medios necesarios. En esta dirección la LPACAP dispone que

«las Administraciones públicas deberán garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios así como los sistemas y aplicaciones que en cada caso se determinen» (art. 12 LPACAP).

#### **2.4. El acceso a la información y los servicios a través de medios electrónicos**

Las personas tienen a su disposición diferentes canales de acceso a las Administraciones públicas a través de medios electrónicos para ejercer sus derechos, 24 horas al día 365 días al año, desde cualquier lugar.

La LRJSP dispone el acceso a la información y a los servicios a través de medios electrónicos mediante:

1) **Punto de acceso electrónico:** es el espacio electrónico a través del que las personas pueden ejercer su derecho a comunicarse con las Administraciones públicas a través de medios electrónicos. El punto de acceso electrónico es un conjunto de páginas web agrupadas en un dominio de internet.

El portal de internet es un punto de acceso electrónico a través del que se facilita acceso a la información publicada por la Administración pública y a la sede electrónica. La titularidad del portal de internet corresponde a una Administración pública, un organismo público o entidad de derecho público.



Además del portal de internet, las Administraciones públicas pueden poner a disposición de los ciudadanos otros puntos de acceso electrónico a través de los que se podrá acceder a las notificaciones o al registro electrónico de cada organismo, por ejemplo.

**2) Sede electrónica:** es la oficina virtual de una Administración pública. La sede electrónica es una dirección electrónica disponible para los ciudadanos a través de las redes de telecomunicaciones mediante la cual las Administraciones públicas difunden información y prestan servicios.

La titularidad, gestión y administración de la sede electrónica corresponden a una Administración pública, órgano o entidad administrativa en el ejercicio de sus competencias. La titularidad de la sede electrónica comporta la responsabilidad con respecto a la integridad, la veracidad y la actualización.

Las sedes electrónicas tienen que disponer de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sea necesario y, además, tienen que garantizar la identificación del titular de la sede.

La información y los servicios que se presten a través de la sede electrónica deben sujetarse a los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, usabilidad, neutralidad e interoperabilidad, y tendrán que tener en cuenta los estándares abiertos y, en su caso, los que sean de uso generalizado por los ciudadanos, así como respetar los principios de accesibilidad y usabilidad.

**3) Otros puntos de acceso electrónico:** además del portal de internet y de la sede electrónica, en la legislación vigente se prevé la puesta a disposición de la ciudadanía de otros puntos de acceso electrónico como el portal de transparencia, el portal de datos abiertos, el perfil de contratante y la ventanilla única.

### 3. El procedimiento administrativo electrónico

El procedimiento administrativo es el cauce formal por medio del cual se producen las resoluciones administrativas. Este procedimiento comprende una serie de actuaciones sucesivas a través de las cuales se conforma la voluntad de las Administraciones públicas.

La nueva regulación del procedimiento administrativo incluida en la LPACAP supone un cambio significativo por lo que respecta al uso de los medios electrónicos. Tal y como se desprende de su preámbulo:

«en el entorno actual, la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos sino que debe constituir la actuación habitual de las Administraciones. Porque una Administración sin papel basada en un funcionamiento íntegramente electrónico no solo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a ciudadanos y empresas, sino que también refuerza las garantías de los interesados».

En efecto, la regulación del procedimiento administrativo llevada a cabo por la LPACAP persigue que toda su tramitación se realice a través de medios electrónicos, independientemente de que el interesado ejerza su derecho a utilizar los medios electrónicos o esté obligado a ello. De este modo, con la entrada en vigor de la LPACAP, el procedimiento administrativo se impulsa en todas sus fases a través de medios electrónicos<sup>9</sup>.

<sup>(9)</sup>Artículo 71.1 LPACAP.

#### 3.1. La identificación y la firma electrónicas

##### 3.1.1. La identificación y la firma electrónicas de los interesados

Las Administraciones públicas deben verificar la identidad de los interesados en el procedimiento administrativo comprobando su nombre y apellidos, o denominación o razón social, de acuerdo con los datos que figuren en el documento nacional de identidad o documento identificativo equivalente. Asimismo, cuando los interesados quieran manifestar su voluntad y consentimiento, así como garantizar la integridad e inalterabilidad del documento, deben firmar los documentos que presenten ante las Administraciones públicas. De hecho, la firma electrónica únicamente será necesaria cuando el interesado quiera formular solicitudes, presentar declaraciones responsables o comunicaciones, interponer recursos, desistir de acciones y renunciar a derechos.

##### **Identificación y firma electrónicas en las Administraciones públicas**

Precisamente, la diferenciación entre la identificación y firma electrónicas es una de las novedades de la LPACAP por la influencia de lo dispuesto en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la

identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Cuando los interesados utilizan los medios electrónicos pueden identificarse ante las Administraciones públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad. En particular, la LPACAP dispone que se podrán utilizar los siguientes mecanismos:

- a) Sistemas basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».
- b) Sistemas basados en certificados electrónicos reconocidos o cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».
- c) Sistemas de clave concertada y cualquier otro sistema que las Administraciones públicas consideren válido, en los términos y condiciones que se establezcan.

Cada Administración pública puede determinar los sistemas que admite para la identificación de los interesados. De todos modos, si se admiten los sistemas previstos en la letra c) conllevará la admisión del resto de sistemas. Asimismo, cuando la Administración General del Estado admita un sistema, este servirá para acreditar la identidad de los interesados ante cualquier Administración pública.

Para la firma electrónica, la LPACAP reconoce que las Administraciones públicas pueden determinar la admisión de los siguientes mecanismos:

- a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».
- b) Sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores de servicios de certificación».
- c) Cualquier otro sistema que las Administraciones públicas consideren válido, en los términos y condiciones que se establezcan.

Cuando un interesado que no esté obligado a utilizar los medios electrónicos no disponga de los mecanismos necesarios para la identificación o la firma electrónica en un procedimiento administrativo, puede dirigirse a una oficina de asistencia en materia de registros para que un funcionario habilitado al

efecto, y ante el que deberá identificarse y prestar su consentimiento expreso, le identifique mediante el sistema de firma electrónico del que esté dotado para ello.

### **3.1.2. La identificación y la firma electrónicas de las Administraciones públicas**

Las Administraciones públicas pueden identificarse mediante el uso de sellos electrónicos basados en un certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Cada Administración pública difundirá la relación de sellos electrónicos utilizados.

La actuación de una Administración pública también puede realizarse mediante la firma electrónica del titular del órgano o empleado público. A tal efecto, cada Administración pública debe determinar los sistemas de firma electrónica que debe utilizar su personal.

Asimismo, cuando la Administración pública actúe de manera automatizada a través de medios electrónicos, es decir, sin la intervención de forma directa de un empleado público, podrá firmar mediante sello electrónico basado en certificado electrónico reconocido o cualificado o código seguro de verificación vinculado a dicha Administración pública.

### **3.2. La iniciación del procedimiento**

El procedimiento administrativo puede iniciarse de oficio o a instancia de persona interesada. Cuando el procedimiento se inicia a instancia de persona interesada, los medios electrónicos adquieren un papel relevante puesto que su escrito deberá presentarse a través de un registro electrónico.

Cada Administración pública debe disponer de un registro electrónico general donde se realizará un asiento de todos los documentos que se presenten o reciban por cada Administración pública. Asimismo, en el registro electrónico también se podrán anotar los documentos que salgan dirigidos a los interesados o a otro órgano administrativo.

El registro electrónico debe crearse a través de una norma que se publicará en el diario oficial correspondiente. La norma de creación deberá concretar el órgano o unidad responsable de su gestión, la fecha y hora oficial y los días declarados como inhábiles<sup>10</sup>.

<sup>(10)</sup>Artículo 16.1 LPACAP.

Desde el punto de vista de la protección de datos, el registro electrónico debe cumplir con las garantías y las medidas de seguridad previstas en la LOPD. Para ello, en las solicitudes normalizadas que las Administraciones públicas pongan a disposición de la ciudadanía, deben constar las obligaciones de obligación previstas.

#### Ejemplo

Por ejemplo, información sobre los derechos de acceso, rectificación, cancelación y oposición o sobre el fichero creado por la Administración pública en el que se incluirán los datos su finalidad, identidad del responsable, etc.

El registro debe garantizar la constancia de los asientos que realice y emitir automáticamente un recibo que consistirá en una copia autenticada del documento de que se trate, incluyendo la fecha y hora de presentación y el número de entrada, así como un recibo acreditativo de los documentos que, en su caso, lo acompañen.

La LPACAP dispone que, cuando un interesado presente de manera presencial un documento, el funcionario de la oficina de asistencia en materia de registros lo digitalizará para incorporarlo al expediente administrativo electrónico y devolverá el original al interesado<sup>11</sup>.

(11) Artículo 16.5 LPACAP.

Los registros electrónicos deben ser plenamente interoperables, para lo que deberá garantizarse la compatibilidad informática y la interconexión entre ellos, así como la transmisión telemática de los asientos registrales y de los documentos entre las Administraciones públicas.

Finalmente, cabe señalar que cuando una incidencia técnica haya imposibilitado el funcionamiento ordinario del registro, y hasta que se solucione el problema, la Administración pública puede determinar una ampliación de los plazos no vencidos, debiendo publicar en la sede electrónica la incidencia técnica acontecida como la ampliación concreta determinada<sup>12</sup>.

(12) Artículo 32.4 LPACAP.

### 3.3. La ordenación del procedimiento administrativo

Las Administraciones públicas deben impulsar de oficio el procedimiento administrativo a través de medios electrónicos<sup>13</sup>.

(13) Artículo 71.1 LPACAP.

La principal novedad que representa el uso de los medios electrónicos, por lo que respecta a la ordenación del procedimiento administrativo, reside en la regulación del expediente electrónico. El expediente es el conjunto ordenado de los documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa. El expediente tiene formato electrónico y se forma mediante la agregación ordenada de los diversos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias que se hayan impulsado, e incluye un índice de todos los documentos que contiene<sup>14</sup>.

(14) Artículo 70 LPACAP.

### 3.4. La instrucción del procedimiento

La instrucción del procedimiento persigue obtener los datos, documentos y pruebas necesarios para la determinación, conocimiento y comprobación de los hechos que sirvan de base para la resolución. La instrucción se realiza de oficio y a través de medios electrónicos<sup>15</sup>.

<sup>(15)</sup>Artículo 75 LPACAP.

Los medios electrónicos pueden ser utilizados por los interesados para presentar sus alegaciones y aportar los documentos u otros elementos de juicio. Asimismo, los medios electrónicos serán usados para la emisión de los informes.

Los documentos públicos electrónicos se emiten por las Administraciones públicas por medios electrónicos y deben incorporar: la información archivada en un soporte electrónico; los datos de identificación que permitan su individualización; una referencia temporal del momento en que se han emitido; metadatos y firmas electrónicas que correspondan.

A lo largo de la tramitación del procedimiento administrativo, las Administraciones públicas pueden realizar copias de los documentos administrativos electrónicos. Las copias auténticas tienen la misma validez y eficacia que los documentos originales<sup>16</sup>. En particular, las copias deben seguir las siguientes reglas:

<sup>(16)</sup>Artículo 27 LPACAP.

- Las copias electrónicas de un documento electrónico original o de una copia electrónica auténtica, con o sin cambio de formato, deben incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.
- Las copias electrónicas de documentos en soporte papel o en otro soporte no electrónico susceptible de digitalización requieren que el documento haya sido digitalizado y deben incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.
- Las copias en soporte papel de documentos electrónicos requieren que en las mismas figure la condición de copia y contener un código generado electrónicamente, u otro sistema de verificación, que permita contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u organismo público emisor.
- Las copias en soporte papel de documentos originales emitidos en dicho soporte se proporcionan mediante una copia auténtica en papel del documento electrónico que se encuentre en poder de la Administración, o bien mediante una puesta de manifiesto electrónica conteniendo copia auténtica del documento original.

### 3.5. La finalización del procedimiento

La forma lógica de finalizar es a través de la resolución que se dicte por parte de la Administración pública y que estará firmada electrónicamente por el titular, órgano o empleado a quien corresponda.

A través de la notificación de la resolución se comunica al interesado su contenido.

Las notificaciones se practican preferentemente a través de medios electrónicos y, en todo caso, cuando el interesado esté obligado a recibirla por esta vía en el plazo de diez días a partir de la fecha en que el acto haya sido dictado<sup>17</sup>.

<sup>(17)</sup>Artículo 41 LPACAP.

Cuando las resoluciones tengan por destinatario a más de un interesado, las Administraciones deben adoptar las medidas necesarias para la protección de los datos personales que consten en las resoluciones y actos administrativos<sup>18</sup>.

<sup>(18)</sup>Artículo 40.5 LPACAP.

Las notificaciones electrónicas se pueden practicar mediante comparecencia en la sede electrónica de la Administración pública actuante o a través de la dirección electrónica habilitada única.

Las notificaciones electrónicas se entenderán practicadas en el momento en que se produzca el acceso a su contenido. Cuando la notificación sea de carácter obligatorio por medios electrónicos o así haya sido elegido por el interesado, la notificación se entenderá rechazada si, en el plazo de diez días desde la puesta a disposición de la notificación, el interesado no ha accedido a su contenido.

Finalmente, con posterioridad a la finalización del procedimiento, los documentos electrónicos deberán conservarse en un archivo electrónico único que mantendrá cada Administración pública. Los documentos se conservarán en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. También se deberán establecer las medidas de seguridad necesarias para garantizar la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados y, en particular, asegurar la identificación de los usuarios y el control de accesos<sup>19</sup>.

<sup>(19)</sup>Artículo 17 LPACAP y artículo 46 LRJSP.

El archivo electrónico deberá asegurar el cumplimiento de las garantías previstas en la legislación de protección de datos. Para ello, se adoptarán las medidas de seguridad previstas en el Esquema Nacional de Seguridad, así como el resto de medidas previstas en el Reglamento de desarrollo LOPD.



## 4. Las especialidades del tratamiento de datos personales en las Administraciones públicas

Las Administraciones públicas recaban grandes cantidades de datos de la ciudadanía en el desarrollo de sus funciones<sup>20</sup>. El uso de estos datos puede generar problemas no solo desde el punto de vista de la seguridad, sino también en la medida en que los medios electrónicos permiten acceder o agregar datos que pueden llegar a facilitar la creación de un perfil de la persona interesada.

<sup>(20)</sup>Por ejemplo, al solicitar una subvención o al pagar impuestos.

Para dar respuesta a todos estos riesgos, tal y como se ha visto anteriormente, la legislación sobre administración electrónica reconoce el derecho a la protección de datos de carácter personal y el derecho a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones públicas y, en particular, prevé el principio de seguridad de la sede electrónica.

El desarrollo de estos derechos y principios se encuentra en la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, así como en el Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de dicha norma. Asimismo, es necesario tener presente 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.

Estas normas prevén determinadas especificidades cuando los tratamientos de datos personales son realizados por Administraciones públicas. En las próximas páginas se presentan las principales especificidades que establece la regulación vigente cuando el responsable del tratamiento es una Administración pública.

### 4.1. La creación de ficheros en las Administraciones públicas

La creación de ficheros en las Administraciones públicas exige la adopción de una disposición general que debe publicarse en el Boletín Oficial del Estado o en el diario oficial correspondiente.

La disposición de creación del fichero debe concretar los siguientes extremos<sup>21</sup>:

<sup>(21)</sup>Artículo 20 LOPD.

- la finalidad del fichero y los usos previstos para él;

- las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos;
- el procedimiento de recogida de los datos de carácter personal;
- la estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo;
- las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros;
- los órganos de las Administraciones responsables del fichero;
- los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición;
- las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

Una vez creado el fichero, la Administración pública debe comunicarlo a la Agencia Española de Protección de Datos o a la autoridad autonómica competente para su inscripción en el Registro General de Protección de Datos.

La modificación o supresión del fichero también debe realizarse a través de una disposición general que nuevamente debe ser publicada en el Boletín Oficial del Estado o en el diario oficial correspondiente.

#### **4.2. Las obligaciones de los responsables del tratamiento. Las relaciones entre los responsables del tratamiento y los encargados del tratamiento**

Desde la perspectiva de la administración electrónica, el responsable del tratamiento es la Administración pública que, sola o junto con otros, determine los fines y medios 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<sup>22</sup>. 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.

<sup>(22)</sup> Artículo 24 RGPD.

Entre estas medidas se encuentra la de elegir un encargado de tratamiento. A pesar de que la responsabilidad última sobre el tratamiento continúa estando atribuida al responsable, debe tenerse en cuenta que el RGPD atribuye obligaciones específicas a los encargados, es decir, a las Administraciones públicas o personas físicas o jurídicas que traten datos personales por cuenta del responsable del tratamiento.

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<sup>23</sup>.

(23) Artículo 28 RGPD.

### 4.3. La adhesión a los códigos de conducta, mecanismos de certificación, normas corporativas vinculantes (BCR)

El RGPD dispone la posibilidad de que los responsables de tratamiento adopten diferentes instrumentos para poder acreditar el cumplimiento de las obligaciones previstas. En particular, 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<sup>24</sup>. De este modo, se facilita y simplifica la aplicación de la normativa en materia de protección de datos personales.

(24) Artículo 24 RGPD.

En primer lugar, se prevé que las Administraciones públicas pueden adoptar códigos de conducta. Asimismo, deben promover la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del RGPD<sup>25</sup>. Los códigos de conducta podrán ser elaborados por asociaciones u organizaciones representativas de categorías de responsables o por encargados de tratamiento.

(25) Artículo 40 RGPD.

#### Responsables de elaborar códigos de conducta

En el ámbito de la Administración local, entidades como la Federación Española de Municipios y Provincias. En 2009, ya se registró el Código Tipo para las entidades locales adheridas a EUDEL.

Los códigos de conducta deben recoger diferentes aspectos relativos a la aplicación del RGPD en relación con la Administración pública que lo adopta. En particular, debe hacer referencia a cuestiones 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<sup>26</sup>.

(26) Artículo 40 RGPD.

El RGPD dispone que el control obligatorio del cumplimiento del código de conducta debe ser realizado por un organismo que tenga el nivel adecuado de pericia y que haya sido acreditado para tal fin por la autoridad de control competente; puede así supervisar el cumplimiento de un código de conducta. Sin embargo, también prevé que las disposiciones relativas a la supervisión de los códigos de conducta no serán aplicables a los tratamientos realizados por las Administraciones públicas<sup>27</sup>.

(27) Artículo 41.6 RGPD.

En segundo lugar, se prevé que las Administraciones públicas 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<sup>28</sup>. Asimismo, las Administraciones públicas, junto con las autoridades de control, promoverán la creación de estos mecanismos de certificación en

(28) Artículo 42 RGPD.

materia de protección de datos. La regulación de las certificaciones no presenta ninguna especificidad por lo que respecta a las Administraciones públicas, motivo por el que nos remitimos al análisis realizado con carácter general.

Finamente, el RGPD prevé la posibilidad de 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<sup>29</sup>.

<sup>(29)</sup>Artículo 47 RGPD.

Asimismo, en el caso de las Administraciones públicas, cuando exista autorización por parte de la autoridad de control competente, las garantías adecuadas pueden ser aportadas mediante disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados. En esta dirección, las transferencias internacionales entre Administraciones públicas de un Estado miembro con Administraciones públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes se podrán realizar sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes, se debe recabar la autorización de la autoridad de control competente.

#### **4.4. La designación y posición del delegado de protección de datos en una Administración pública**

El responsable y el encargado del tratamiento deben designar un delegado de protección de datos siempre que el tratamiento lo lleve a cabo una Administración pública<sup>30</sup>. Cuando el responsable o el encargado del tratamiento sea una Administración pública, se puede designar un único delegado de protección de datos para varias Administraciones públicas u organismos, teniendo en cuenta su estructura organizativa y tamaño.

<sup>(30)</sup>Artículo 37 RGPD.

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 tendrá como mínimo las siguientes funciones<sup>31</sup>:

<sup>(31)</sup>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<sup>32</sup>. Asimismo, deben garantizar que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. Además, no podrá ser destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

<sup>(32)</sup>Artículo 38 RGPD.

#### **4.5. Régimen sancionador aplicable a las Administraciones públicas**

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<sup>33</sup>. 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.

<sup>(33)</sup>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<sup>34</sup>.

<sup>(34)</sup> Artículo 83.7 RGPD.

## 5. El gobierno abierto y la protección de datos personales

El gobierno abierto persigue el fortalecimiento de las relaciones entre las Administraciones públicas y la ciudadanía a través de la transparencia, la participación y la colaboración ciudadana a través del uso intensivo de los medios electrónicos.

El gobierno abierto facilita que las Administraciones públicas puedan escuchar las preferencias de la ciudadanía y esta pueda manifestar su opinión implicándole en el diseño y la implementación de las políticas públicas.

En los últimos años el gobierno abierto ha ido adquiriendo gran importancia gracias, entre otros elementos, a la extensión de los medios electrónicos, especialmente de las tecnologías incluidas bajo la etiqueta 2.0 que facilitan la escucha activa y la participación ciudadana en las Administraciones públicas.

De todos modos, el gobierno abierto va más allá del uso de la tecnología en las relaciones entre las Administraciones públicas y la ciudadanía. También implica un cambio de valores en las Administraciones públicas impulsado por la innovación.

La transparencia pública es el primer pilar del gobierno abierto y en él se centrará la atención en este módulo. La transparencia persigue facilitar que la ciudadanía tenga un conocimiento efectivo de lo que sucede en el seno de las oficinas públicas. Además, la transparencia tiene otras finalidades, como se desprende de la lectura del preámbulo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno:

«Solo cuando la acción de los responsables públicos se somete a escrutinio, cuando los ciudadanos pueden conocer cómo se toman las decisiones que les afectan, cómo se manejan los fondos públicos o bajo qué criterios actúan nuestras instituciones podremos hablar del inicio de un proceso en el que los poderes públicos comienzan a responder a una sociedad que es crítica, exigente y que demanda participación de los poderes públicos.

Los países con mayores niveles en materia de transparencia y normas de buen gobierno cuentan con instituciones más fuertes, que favorecen el crecimiento económico y el desarrollo social. En estos países, los ciudadanos pueden juzgar mejor y con más criterio la capacidad de sus responsables públicos y decidir en consecuencia. Permitiendo una mejor fiscalización de la actividad pública se contribuye a la necesaria regeneración democrática, se promueve la eficiencia y eficacia del Estado y se favorece el crecimiento económico.»

### Lectura recomendada

L. Cotino Hueso (2013). «Derecho y “Gobierno Abierto”. La regulación de la transparencia y la participación y su ejercicio a través del uso de las nuevas tecnologías y las redes sociales por las Administraciones públicas. Propuestas concretas». *Monografías de la Revista Aragonesa de Administración Pública* (núm. XIV, págs. 51-92).

El cumplimiento de las obligaciones de transparencia exige un cambio en la forma como se gestiona, almacena y recupera la información para facilitar no solo una mayor eficacia y eficiencia administrativa, sino para contribuir al incremento de la transparencia pública. En esta dirección, hay que incorporar las obligaciones de transparencia dentro del ciclo de vida documental, de manera que se garantice el acceso efectivo de la ciudadanía a la información pública, permitiendo además la trazabilidad de los documentos hasta la fuente de origen a través de la transparencia por diseño (Cerrillo y Casadesús, 2016).

La transparencia se canaliza a través de diferentes mecanismos: la difusión de información pública (transparencia activa), el acceso a la información pública (transparencia pasiva) y la reutilización de la información pública (transparencia colaborativa).

### 5.1. La difusión de información pública

La difusión de información pública consiste en la puesta a disposición de la ciudadanía de información por parte de las Administraciones públicas, generalmente a través de internet.

De acuerdo con la Ley 19/2013, de 9 de diciembre, las Administraciones públicas deben difundir, como mínimo, información relativa a:

1) **Información institucional, organizativa y de planificación.** Las Administraciones públicas tienen que difundir información sobre las funciones que desarrollan las Administraciones públicas y los planes y programas anuales y plurianuales.

2) **Información de relevancia jurídica.** Las Administraciones públicas, en el ámbito de sus competencias, tienen que publicar las directrices, instrucciones, acuerdos, circulares o respuestas a consultas planteadas; los anteproyectos de ley y los proyectos de decretos legislativos; los proyectos de reglamentos y las memorias e informes que conforman los expedientes de elaboración de los textos normativos.

3) **Información económica, presupuestaria y estadística.** Las Administraciones públicas también tienen que difundir información detallada relativa a los contratos públicos; la relación de los convenios suscritos; las subvenciones y ayudas públicas concedidas; los presupuestos; las cuentas anuales; las retribuciones percibidas anualmente por los altos cargos; las resoluciones de autorización o reconocimiento de compatibilidad que afecten a los empleados públicos; las declaraciones anuales de bienes y actividades de los representantes locales; la información estadística necesaria para valorar el grado de cumplimiento y calidad de los servicios públicos.

#### Referencia bibliográfica

A. Cerrillo Martínez; A. Casadesús (2016). *La transparencia por diseño: el impacto de la gestión documental en la transparencia pública*.



**4) Información de interés general.** Además de toda esta información que tienen que difundir las Administraciones públicas por medios electrónicos, un análisis de los portales y páginas web de la mayoría de las Administraciones públicas muestra que generalmente también se difunde mucha otra información de interés para la ciudadanía.

La información pública debe difundirse a través de páginas web o sedes electrónicas. En particular, la legislación de transparencia ha previsto que las Administraciones públicas difundan la información a través de portales de transparencia. Sin embargo, únicamente se concretan las características en relación al Portal de Transparencia de la Administración General del Estado, que deberá adecuarse a los principios de accesibilidad, interoperabilidad y reutilización.

Todas las leyes autonómicas prevén que la información estará disponible a través de un portal de transparencia. Las diferentes leyes prevén sistemas diversos como difundir información de todos los sujetos obligados, aunque en general persiguen la difusión de información no únicamente de la Administración autonómica, por ejemplo, a través de la integración de la información (Cataluña), a través de la interoperabilidad y el intercambio de la información (Aragón o Región de Murcia), mediante enlaces electrónicos a la ubicación de la información (Aragón) o a través de otros mecanismos de colaboración (Comunidad Valenciana).

La información que difunden las Administraciones públicas debe ser de calidad para que pueda cumplir las finalidades previstas (Cerrillo y Galán, 2007). Para conseguir estas finalidades, es necesario que la información que se difunda sea actualizada, objetiva, útil y accesible. Asimismo, incide en la calidad de la información la seguridad y la autenticidad de su autoría, así como la integridad de su contenido. También se prevé que

«la información sujeta a las obligaciones de transparencia será publicada en las correspondientes sedes electrónicas o páginas web y de una manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada así como su identificación y localización» (art. 5.5 LTAIBG).

## 5.2. El acceso a la información pública

El acceso a la información consiste en la solicitud a una Administración pública por parte de cualquier persona para que se les muestre una determinada información o se les facilite una copia de la misma. El acceso a la información es un derecho subjetivo que reconoce la legislación vigente<sup>35</sup>.

La LTAIBG prevé que se entiende por información pública «los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones»<sup>36</sup>.

### Referencia bibliográfica

A. Cerrillo Martínez; A. Galán Galán (2007). *Qualitat i responsabilitat en la difusió d'informació pública a Internet*. Barcelona: Escola d'Administració Pública de Catalunya i Generalitat de Catalunya.

<sup>(35)</sup>Artículo 12 LTAIBG.

<sup>(36)</sup>Artículo 13 LTAIBG.

El derecho de acceso a la información se ejerce mediante una solicitud que se puede presentar por cualquier medio que permita tener constancia de la identidad del solicitante, la información que solicita, la dirección de contacto –preferentemente electrónica– y la modalidad que se prefiera para acceder a la información solicitada. El solicitante no está obligado a motivar su solicitud. Para facilitar el acceso a la información pública, la mayoría de Administraciones públicas están poniendo a disposición de la ciudadanía formularios electrónicos de solicitud de información. Para poderlos utilizar requieren el uso de sistemas de firma electrónica lo que con frecuencia se acaba convirtiendo en un freno al ejercicio del derecho de acceso<sup>37</sup>.

(37) Véase: [http://transparencia.gob.es/transparencia/transparencia\\_Home/index/Derecho-de-acceso-a-la-informacion-publica/Solicite-informacion.html](http://transparencia.gob.es/transparencia/transparencia_Home/index/Derecho-de-acceso-a-la-informacion-publica/Solicite-informacion.html)

La LTAIBG prevé diferentes causas de inadmisión de las solicitudes:

- que se refieran a información que esté en curso de elaboración o de publicación general<sup>38</sup>.
- que se refieran a información que tenga carácter auxiliar o de apoyo como la contenida en notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas<sup>39</sup>.
- que se refieran a información para cuya divulgación sea necesaria una acción previa de reelaboración<sup>40</sup>.
- que estén dirigidas a un órgano en cuyo poder no obre la información cuando se desconozca el competente.
- que sean manifiestamente repetitivas o tengan un carácter abusivo no justificado con la finalidad de transparencia<sup>41</sup>.

(38) Véanse al respecto los criterios interpretativos 7/2015 y 9/2015, de 12 de noviembre, del Consejo de Transparencia y Buen Gobierno.

(39) Véase al respecto el criterio interpretativo 6/2015, de 12 de noviembre, del Consejo de Transparencia y Buen Gobierno.

(40) Véase al respecto el criterio interpretativo 7/2015, de 12 de noviembre, del Consejo de Transparencia y Buen Gobierno.

(41) Véase al respecto el criterio 3/2016, de 14 de julio, del Consejo de Transparencia y Buen Gobierno.

En la tramitación del procedimiento se concederá un plazo a terceras personas cuyos derechos o intereses puedan verse afectados por el acceso a la información.

El procedimiento se resolverá y notificará en el plazo máximo de un mes desde la recepción de la solicitud por el órgano competente para resolver. En el caso de que la resolución deniegue el acceso, conceda el acceso parcial o a través de una modalidad distinta de la solicitada, deberá motivarse. Transcurrido el plazo sin que se haya dictado y notificado la resolución deberá entenderse desestimada<sup>42</sup>.

(42) En relación con el carácter del silencio debe tenerse presente que algunas normas autonómicas prevén el silencio positivo (Aragón, Cataluña o Navarra).

La LTAIBG prevé que, contra toda resolución expresa o presunta en materia de acceso a la información, se puede interponer, con carácter potestativo y previo a la impugnación en vía contencioso-administrativa, una reclamación ante el Consejo de Transparencia y Buen Gobierno u órgano independiente que determinen las comunidades autónomas. Esta reclamación se puede interponer en el plazo de un mes y se debe ajustar a lo dispuesto en la LPACAP,

dándose trámite de audiencia a las personas que pudieran resultar afectadas por el acceso. El plazo máximo para resolver y notificar la resolución será de tres meses, transcurrido el cual la reclamación se entenderá desestimada.

### **El Consejo de Transparencia y Buen Gobierno**

El Consejo de Transparencia y Buen Gobierno es un organismo público con autonomía y plena independencia en el cumplimiento de sus fines adscrito al Ministerio de Hacienda y Administraciones Públicas.

El Consejo de Transparencia y Buen Gobierno está compuesto por la Comisión de Transparencia y Buen Gobierno y el presidente del Consejo de Transparencia y Buen Gobierno. La Comisión está formada por el presidente, un diputado, un senador, un representante del Tribunal de Cuentas, un representante del defensor del pueblo, un representante de la Agencia Española de Protección de Datos, un representante de la Secretaría de Estado de Administraciones Públicas y un representante de la Autoridad Independiente de Responsabilidad Fiscal. Por su parte, el presidente del Consejo de Transparencia y Buen Gobierno es nombrado por un periodo no renovable de cinco años por el Gobierno, entre personas de prestigio reconocido y competencia profesional después de que la persona propuesta para el cargo comparezca ante la comisión correspondiente del Congreso de los Diputados.

Algunas comunidades autónomas han asumido esta competencia y han creado órganos u organismos independientes a las que han atribuido la función de resolver las reclamaciones, así como, en algunos casos, otras funciones como evaluar el cumplimiento de las obligaciones de transparencia o la protección de los datos personales (Andalucía, Aragón, Castilla y León, Canarias, Cataluña, Comunidad Valenciana, Galicia, Islas Baleares, La Rioja, Navarra, Región de Murcia). En algunos casos, se les han atribuido funciones de mediación para la resolución de los conflictos que puedan surgir en materia de acceso a la información pública (Cataluña).

### **5.3. La reutilización de información pública**

El gobierno abierto se basa en la apertura de datos y su reutilización. En efecto, el acceso libre y gratuito a la información pública favorece la participación y la colaboración ciudadana a través de la reutilización de la información pública.

La reutilización consiste en el uso de documentos que están en poder de las administraciones y organismos del sector público, por parte de personas físicas o jurídicas, con finalidades comerciales o no comerciales, siempre que este uso no constituya una actividad administrativa pública, ni tampoco el intercambio de documentos entre administraciones públicas en el ejercicio de las funciones públicas que tengan atribuidas<sup>43</sup>. En particular, puede ser objeto de reutilización toda información, sea cual sea su soporte y forma de expresión, elaborada o custodiada por las Administraciones públicas y organismos públicos. Sin embargo, la LRISP excluye del régimen de reutilización previsto los documentos que no sean accesibles, aquellos cuyo conocimiento requiera una legitimación especial y los contenidos públicos creados, por ejemplo, por entidades de radiodifusión o entidades educativas.

<sup>(43)</sup>Artículo 3 LRISP.

La LRISP recoge la obligación para las Administraciones y organismos del sector público de autorizar la reutilización de los documentos al prever que «los documentos de las Administraciones públicas y organismos del sector público son reutilizables en los términos que prevé esta Ley» y remitirse a los regímenes determinados por cada Administración pública<sup>44</sup>.

(44) Artículo 4 LRISP.

La LRISP define tres modalidades de reutilización, entre las cuales puede optarse Administración pública al definir el régimen jurídico específico de la reutilización de la información:

- Reutilización sin sujeción a condiciones.
- Reutilización con sujeción a condiciones establecidas en licencias tipo, que tienen que estar disponibles en formato digital y deben ser procesables de manera electrónica.
- Reutilización con solicitud previa, que puede incorporar condiciones en una licencia; esta licencia tiene que reflejar, al menos, la información relativa a la finalidad concreta, comercial o no comercial, por la cual se concede la reutilización, la duración de la licencia, las obligaciones del beneficiario y del organismo concedente, las responsabilidades de uso y las modalidades financieras, por lo cual se tiene que indicar el carácter gratuito o, si procede, la contraprestación económica aplicable.

Las condiciones incorporadas en las licencias deben: ser claras, justas y transparentes; no restringir las posibilidades de reutilización ni limitar la competencia; no ser discriminatorias para categorías comparables de reutilización; y no contener acuerdos exclusivos.

Estas condiciones pueden referirse a que el contenido de la información, incluyendo sus metadatos, no sea alterado; no se desnaturalice el sentido de la información; se cite la fuente; se mencione la fecha de la última actualización; la finalidad o finalidades concretas para las que es posible la reutilización futura de los datos cuando la información contenga datos de carácter personal.

En particular, resulta de interés señalar que entre las condiciones de la reutilización se puede prever la prohibición de revertir el procedimiento de disociación mediante la adición de nuevos datos obtenidos de otras fuentes cuando la información, aun siendo facilitada de forma disociada, contuviera elementos suficientes que pudieran permitir la identificación de los interesados en el proceso de reutilización<sup>45</sup>.

(45) Artículo 8.f) LRISP.

A través de la apertura de datos públicos se favorece la reutilización de la información pública al facilitar la creación de información y la oferta de nuevos servicios de valor añadido basados en los datos difundidos por las Administraciones públicas. En esta dirección, la Comisión Europea, afirma que

«el impulso hacia la utilización de datos abiertos está cobrando fuerza en varios Estados miembros, los cuales están adoptando este concepto por razones de transparencia, eficiencia administrativa y potencial económico de la reutilización» (Comisión Europea, 2011).

Los datos públicos que se ponen a disposición de los ciudadanos deben cumplir determinadas características que persiguen garantizar que se puedan reutilizar fácilmente para generar nuevas informaciones o servicios que, en última instancia, pueden incrementar la transparencia de las Administraciones públicas.

Los datos abiertos se caracterizan, desde un punto de vista técnico, por ser procesables electrónicamente y, desde el punto de vista jurídico, por la ausencia de restricciones que limiten su reutilización (propiedad intelectual, datos personales, etc.). De acuerdo con la Sunlight Foundation, los datos abiertos son aquellos datos completos, primarios, oportunos, accesibles de forma física y electrónica, procesables electrónicamente, no discriminatorios que usan estándares abiertos en la difusión, sin licencia, permanentes y sin costes<sup>46</sup>.

<sup>(46)</sup>Véase en: <https://sunlightfoundation.com/wp-content/uploads/2016/11/Ten-Principles-for-Opening-Up-Government-Data.pdf> (última consulta: mayo de 2017).

La LRISP, después de la modificación operada por la Ley 18/2015, de 9 de julio, dispone lo siguiente:

«2. Las Administraciones y organismos del sector público facilitarán sus documentos en cualquier formato o lengua preexistente, pero también procurarán, siempre que ello sea posible y apropiado, proporcionarlos en formato abierto y legible por máquina conforme a lo previsto en el apartado anterior y conjuntamente con sus metadatos, con los niveles más elevados de precisión y desagregación. Tanto el formato como los metadatos, en la medida de lo posible, deben cumplir estándares y normas formales abiertas.»

De este modo, la LRISP prevé que, cuando sea posible, las Administraciones públicas deben facilitar los datos abiertos para facilitar su reutilización. De todos modos, a pesar de la dicción de este precepto, es importante tener presente que si bien las Administraciones públicas deben tratar de difundir sus datos en formato abierto y promover que la puesta a disposición de los datos para su reutilización se realice por medios electrónicos y mediante plataforma multi-canal, no tienen la obligación de difundir los datos en dicho formato.

Diversas normas autonómicas prevén que las Administraciones públicas deberán promover la difusión de los datos públicos en formatos abiertos (Castilla-La Mancha, Galicia, Aragón, Región de Murcia, Andalucía y Extremadura). Asimismo, disponen la creación de portales de datos abiertos o de secciones específicas al efecto en los portales de transparencia con la finalidad de favorecer la reutilización (Castilla-La Mancha y Aragón). También prevén la creación de catálogos de información reutilizable (Galicia y La Rioja).

La LRISP establece diferentes infracciones, como: la desnaturalización del sentido de la información, para cuya reutilización se haya concedido una licencia; la alteración del contenido de la información para cuya reutilización se haya concedido una licencia o la reutilización de documentación sin haber obtenido la correspondiente licencia en los casos en los que esta sea requerida o incumpliendo las condiciones impuestas en la correspondiente licencia o en la normativa reguladora aplicable. La LRISP prevé que, por la comisión de las anteriores infracciones, se pueden imponer diferentes sanciones de multa además de la prohibición de reutilizar documentos sometidos a licencia durante un periodo de entre uno y cinco años, y con la revocación de la licencia concedida. Este régimen sancionador únicamente es aplicable en relación con la Administración General del Estado.

#### **5.4. La protección de datos personales como límite a la transparencia pública**

La LTAIBG dispone que la transparencia podrá ser limitada cuando el conocimiento o el acceso a la información pueda suponer un perjuicio a una serie de bienes o derechos como la seguridad nacional, la defensa, las relaciones exteriores, la seguridad pública, la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios, la igualdad de las partes en los procesos judiciales y la tutela judicial efectiva, las funciones administrativas de vigilancia, inspección y control, los intereses económicos y comerciales, la política económica y monetaria, el secreto profesional y la propiedad intelectual e industrial y la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión y la protección del medio ambiente.

Asimismo, la LTAIBG prevé que, si la información solicitada contiene datos personales, únicamente se podrá autorizar el acceso en determinadas circunstancias a las que se hará referencia a continuación.

La concurrencia de uno de estos bienes o derechos en la información que se quiera difundir, o a la que una persona quiera acceder, no determina en sí mismo la imposibilidad de su conocimiento público. En efecto, en la aplicación de los límites, cabe tener en cuenta diversos elementos.

En primer lugar, las Administraciones públicas no disponen de potestad discrecional para denegar o limitar el acceso a la información pública<sup>47</sup>.

<sup>(47)</sup>Véase al respecto lo previsto en el artículo 20.3 Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno de Cataluña.

En segundo lugar, la concurrencia de un interés o derecho protegido por un límite no supone, obligatoriamente, la denegación del acceso a la información pública. Es esta dirección, el Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos recuerdan que «los límites no operan ni automáticamente a favor de la denegación ni absolutamente en relación con los contenidos»<sup>48</sup>.

<sup>(48)</sup>Criterio interpretativo 2/2015, de 24 de junio.

En tercer lugar, el perjuicio debe ser cierto e inequívoco. Para poder determinar el perjuicio que el conocimiento de la información pueda generar, las Administraciones públicas pueden utilizar diferentes criterios:

- **Test del daño:** la Administración pública debe valorar el daño que el acceso puede producir al bien o interés protegido por el límite. La aplicación del límite debe ser justificada y proporcionada a su objeto y finalidad perseguida con la protección y atenderá a las circunstancias del caso concreto<sup>49</sup>.
- **Test del interés público:** la Administración pública debe realizar una aplicación justificada y proporcional del límite atendiendo a la circunstancia del caso concreto y siempre que no exista un interés que justifique la publicidad o el acceso.
- **Test de ponderación de intereses:** la Administración pública debe ponderar si concurre un interés público o privado superior que justifique el acceso.

<sup>(49)</sup>Artículo 14.2 LTAIBG.

La protección de los datos personales constituye la principal causa de denegación del acceso a la información pública.

### **Transparencia y protección de datos en el RGPD**

El RGPD reconoce que en su aplicación se debe tener en cuenta el derecho de acceso a la información pública. En particular, con carácter general se establece que «los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo». Para ello, es necesario «conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales y, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales» (Considerando 154 RGPD).

De todos modos, este reconocimiento no puede afectar o alterar la protección de datos personales. Como concreción de esta idea, se puede traer a colación lo que ya establecía la Directiva 2003/98/CE del Parlamento Europeo y del Consejo al afirmar que «la presente Directiva se debe incorporar al derecho interno y aplicar de forma que se cumplan plenamente los principios relativos a la protección de los datos personales, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de

1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos».

En esta dirección, el RGPD dispone que los datos personales de documentos oficiales en posesión de cualquier Administración pública pueden ser comunicados de conformidad con la regulación aplicable para conciliar el acceso del público a documentos oficiales y el derecho a la protección de los datos personales (art. 86 RGPD).

El equilibrio entre la transparencia y la protección de datos es complejo, como se desprende de la lectura de la doctrina de los órganos de garantía del derecho de acceso a la información pública.

Para dar respuesta a esta situación, La LTAIBG establece las siguientes normas para determinar si la información que contiene datos personales puede ser difundida o no:

- si la información contiene datos especialmente protegidos relativos a la ideología, afiliación sindical, religión o las creencias, podrá autorizar el acceso si el afectado ha manifestado su consentimiento expreso y por escrito, a menos que haya hecho manifiestamente públicos los datos con anterioridad a la solicitud de acceso;
- si la información contiene datos especialmente protegidos relativos al origen racial, a la salud y a la vida sexual o a la comisión de infracciones penales o administrativas, el acceso solo se podrá autorizar si el afectado ha manifestado su consentimiento expreso o si está amparado con una norma con rango de ley;
- si la información contiene datos personales pero no son especialmente protegidos, se deberá conceder el acceso previa ponderación entre el interés público en la difusión de la información y los derechos del afectado. En esta ponderación se tendrán en cuenta: el menor perjuicio derivado del transcurso del tiempo; la justificación de la solicitud; la condición de investigador del solicitante y que el acceso se base en fines históricos, científicos o estadísticos; el menor perjuicio de los derechos de los afectados porque los documentos únicamente contienen datos meramente identificativos; la mayor garantía de los derechos del afectado en el caso que los datos puedan afectar a su intimidad o seguridad o se refieran a menores de edad;
- si la información contiene datos personales meramente identificativos relacionados con la organización, funcionamiento o actividad del órgano se concederá el acceso a la información, salvo que en el caso concreto prevalezca la protección de los datos sobre el interés público. Estos datos son aquellos que únicamente facilitan información para determinar la identidad de la persona física (nombre y apellidos, DNI, cargo, teléfono, dirección de correo electrónico...), siempre y cuando estén vinculados con la organización, funcionamiento o actividad del órgano administrativo.

#### **Derecho de acceso LTAIBG y derecho de acceso LOPD**

La LTAIBG no hace ninguna mención específica al ejercicio del derecho de acceso para acceder a los datos personales del solicitante. Al respecto, debe tenerse presente que el solicitante puede ejercer el derecho de acceso previsto en la LOPD, que va acompañado del derecho de rectificación y cancelación y cuenta con la garantía ante la agencia de protección de datos competente. Sin embargo, no se puede desconocer el alcance del derecho de acceso regulado en la LOPD. En efecto, esta norma dispone que «el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos» (art. 15 LOPD). Pero no se concreta que pueda acceder a los datos en sí mismos. Por ello, como advierten Fernández Ramos y Pérez Monguió, «si el titular de los datos quiere acceder a la información pública en su integridad, debe poder ejercitar el derecho de acceso, como cualquier otra persona, pues de lo contrario sería tratado de peor condición que un tercero, por completo ajeno a la información pública» (Fernández Ramos y Pérez Monguió, 2017, pág. 198).

<sup>(50)</sup> Artículo 15.5 LTAIBG.



Cuando finalmente se facilita el acceso a información que contiene datos personales, es importante tener presente que la normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso<sup>50</sup>.

De todos modos, la propia LTAIBG señala que no será de aplicación lo anterior si se disocian los datos personales de la información solicitada de manera que no pueda ser posible la identificación de los afectados. La disociación de los datos personales es aquel tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable, es decir, que permita obtener un dato disociado.

La disociación o anonimización persigue eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de estos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales<sup>51</sup>. De acuerdo con la Agencia Española de Protección de Datos, hay que garantizar la irreversibilidad de la anonimización, y para ello deberán valorar tanto las fuentes de información disponibles en los diferentes medios y, en particular, a través de internet, como la tecnología aplicable en los procesos de anonimización y en los de reidentificación.

<sup>(51)</sup>Véase al respecto las Orientaciones y garantías en los procedimientos de anonimización de datos personales de la Agencia Española de Protección de Datos de 2016.

### La anonimización

La anonimización se puede llevar a cabo utilizando diferentes técnicas. Según el Dictamen 05/2014 sobre técnicas de anonimización del Grupo de Trabajo sobre Protección de Datos del artículo 29, se pueden utilizar técnicas de anonimización como la aleatorización (adición de ruido, la permutación, la privacidad diferencial), la generalización (agregación, anonimato k, diversidad de proximidad) y la pseudonimización (cifrado de clave secreta, función *hash*). Sin embargo, estas técnicas pueden generar riesgos de singularización (posibilidad de extraer de los datos registros que identifican a una persona), vinculabilidad (capacidad de vincular dos o más registros de una persona de una o varias bases de datos) o inferencia (posibilidad de deducir el valor de un atributo a partir de los valores del resto de atributos). Para reducir los riesgos de identificación se pueden seguir unas buenas prácticas, tales como evaluar periódicamente los riesgos, no olvidar la posibilidad de que haya atacantes, utilizar de manera combinada diversas técnicas o revelar la técnica utilizada (Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2014).

Finalmente, en la medida en que la aplicación de los límites del derecho de acceso se ha de realizar de forma proporcional a su objeto y finalidad de protección y atender a las circunstancias del caso concreto y ser justificada, si un límite afecta únicamente a una parte de la información solicitada, se facilitará el acceso restringido a aquellos datos que no se vean afectados por el mismo salvo que de ello resulte una información distorsionada o que carezca de sentido<sup>52</sup>.

<sup>(52)</sup>Artículo 16 LTAIBG.

## 6. Las relaciones interadministrativas por medios electrónicos. Las comunicaciones de datos entre Administraciones públicas

### 6.1. La cooperación interadministrativa por medios electrónicos

Los medios electrónicos pueden facilitar las relaciones interadministrativas además de ser un instrumento útil para fomentar la administración electrónica. En efecto, las relaciones interadministrativas constituyen uno de los principales motores para facilitar el desarrollo de la administración electrónica (Cerrillo Martínez, 2010a, pág. 757).

Las Administraciones públicas se deben relacionar entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos<sup>53</sup>.

<sup>(53)</sup> Artículo 3.2 LRJSP.

Los medios electrónicos que utilicen las Administraciones públicas para relacionarse deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptados por cada una de ellas<sup>54</sup>. Asimismo, deben garantizar la protección de los datos de carácter personal.

<sup>(54)</sup> Artículo 3.2 LRJSP.

Para conseguir la comunicación entre administraciones a través de medios electrónicos es necesario garantizar la interoperabilidad, de manera que los sistemas de información de las diversas Administraciones públicas puedan efectivamente interconectarse e intercambiar información.

La interoperabilidad es la capacidad de los sistemas de información, y de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos<sup>55</sup>. La interoperabilidad permite que las Administraciones públicas puedan comunicar, interpretar e intercambiar datos. Para ello, es necesario que definan y compartan unos estándares comunes. En particular, el Esquema Nacional de Interoperabilidad comprende el conjunto de criterios y recomendaciones, en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad<sup>56</sup>. El Esquema Nacional de Interoperabilidad se basa en los principios de integralidad, multidimensionalidad y multilateralidad, y para su implementación prevé diferentes instrumentos como el Inventario de procedimientos administrativos y servicios, la Relación de modelos de datos de intercambio, el Catálogo de estándares y especificaciones técnicas, así como las Normas técnicas de interoperabilidad, que serán de obligado cumplimiento<sup>57</sup>. Las Normas

<sup>(55)</sup> Preámbulo Real decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.

<sup>(56)</sup> Artículo 156.1 LRJSP. El Esquema Nacional de Interoperabilidad se incluye en el Real decreto 4/2010, de 8 de enero.

<sup>(57)</sup> Véanse las normas técnicas sobre interoperabilidad en [http://administracionelectronica.gob.es/pae\\_Home/pae\\_Estrategias/pae\\_Interoperabilidad\\_Inicio/pae\\_Normas\\_tecnicas\\_de\\_interoperabilidad.html](http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html).

<sup>(58)</sup> Disposición adicional primera Esquema Nacional de Interoperabilidad.

técnicas de interoperabilidad son aprobadas por el Ministerio de la Presidencia, a propuesta de la Comisión Sectorial de Administración Electrónica, y son de obligado cumplimiento por las Administraciones públicas<sup>58</sup>.

Las administraciones pueden poner a disposición del resto de Administraciones públicas las aplicaciones desarrolladas por sus servicios o que hayan sido desarrolladas por terceros y de cuyos derechos de propiedad intelectual sean titulares. La reutilización de sistemas y aplicaciones constituye un instrumento para fomentar la interoperabilidad, además de suponer un mecanismo para conseguir una mayor eficiencia y ahorro en el desarrollo de la administración electrónica. La LRJSP prevé que las Administraciones públicas podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas<sup>59</sup>.

(<sup>59</sup>) Artículo 157.1 LRJSP.

El Esquema Nacional de Interoperabilidad determina las condiciones de licenciamiento aplicables a las aplicaciones con el fin de facilitar el aprovechamiento y la reutilización. En particular, se dispone que las Administraciones públicas utilizarán aplicaciones de fuentes abiertas bajo licencias que aseguren que pueden ejecutarse para cualquier propósito; permiten conocer su código fuente; pueden modificarse o mejorarse; pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas mismas cuatro garantías<sup>60</sup>.

(<sup>60</sup>) Artículo 16 Esquema Nacional de Interoperabilidad.

La LRJSP dispone que las Administraciones públicas, antes de adquirir, desarrollar o mantener una aplicación, deberá consultar en el directorio general de aplicaciones si existen soluciones disponibles para su reutilización<sup>61</sup>.

(<sup>61</sup>) Artículo 157.3 LRJSP.

Las Administraciones públicas mantendrán directorios actualizados de aplicaciones para su libre reutilización, de conformidad con lo dispuesto en el Esquema Nacional de Interoperabilidad. Los directorios de las diferentes Administraciones públicas deben ser compatibles y estar interconectados, en particular, con el directorio general de la Administración General del Estado.

(<sup>62</sup>) Artículo 158.2 LRJSP y artículo 17 Esquema Nacional de Interoperabilidad.

La Administración General del Estado debe mantener disponible en dicho directorio aplicaciones en el que constarán tanto las aplicaciones disponibles de la Administración General del Estado como las disponibles en los directorios integrados de aplicaciones del resto de administraciones<sup>62</sup>. El Centro de Transferencia de Tecnología es el portal donde la Administración publica su directorio general de aplicaciones para favorecer la reutilización de soluciones por todas las administraciones públicas<sup>63</sup>.

(<sup>63</sup>) Véase en: <http://administracionelectronica.gob.es/ctt/> (última consulta: mayo de 2017).

En el caso de que exista una solución disponible, las Administraciones públicas estarán obligadas a su uso salvo que la no reutilización sea más eficiente, y así se justifique<sup>64</sup>.

(<sup>64</sup>) Artículo 157.3 LRJSP.

La Administración General del Estado debe prestar apoyo para la libre reutilización de las aplicaciones. La Administración estatal también debe impulsar el desarrollo de aplicaciones, formatos y estándares comunes en el marco de los esquemas de interoperabilidad y seguridad<sup>65</sup>.

(<sup>65</sup>) Artículo 158.2 LRJSP.

Finalmente, la LRJSP prevé la creación de la Comisión Sectorial de Administración Electrónica, dependiente de la Conferencia Sectorial de Administración Pública. Esta comisión sectorial es el órgano técnico de cooperación de la Administración General del Estado, de las Administraciones de las comunidades autónomas y de las Entidades locales en materia de administración electrónica. A esta comisión le corresponde: asegurar la compatibilidad e interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones públicas; impulsar el desarrollo de la administración electrónica en España; y, en última instancia, asegurar la cooperación entre las Administraciones públicas para proporcionar información administrativa clara, actualizada e inequívoca<sup>66</sup>.

<sup>(66)</sup> Disposición adicional novena LRJSP.

## 6.2. Las comunicaciones de datos entre Administraciones públicas

Las Administraciones públicas deben intercambiar datos para el desarrollo de sus actividades.

La comunicación de datos entre Administraciones públicas constituye una manifestación del principio de simplificación, así como una base sobre la que los interesados pueden ejercer su derecho a no presentar datos y documentos que ya se encuentren en poder de las Administraciones públicas o que hayan sido elaborados por estas<sup>67</sup>. Asimismo, mejora la eficacia y la cooperación y coordinación administrativa. La cooperación interadministrativa es necesaria para conseguir plenamente los beneficios que se derivan del uso intensivo de los medios electrónicos por las Administraciones públicas (Cerrillo Martínez, 2010a).

<sup>(67)</sup> Art. 53.1.d) LPACAP.

En los últimos años se ha potenciado la transmisión de datos entre Administraciones públicas y, en su seno, entre órganos y entidades públicas a través de entornos cerrados de comunicación. Así, en la actualidad es posible, a través de este mecanismo, verificar y consultar, entre otros, los datos relativos a la identidad (Dirección General de la Policía), la situación de desempleo (Servicio Público de Empleo Estatal), el alta y si una persona está al corriente de pago en la Seguridad Social (Tesorería General de la Seguridad Social) o si una entidad está al corriente de pago de las obligaciones tributarias (Agencia Estatal de Administración Tributaria). De hecho, la Plataforma de Intermediación de Datos ha tenido más de 4.300.000 transacciones en un mes (abril de 2016)<sup>68</sup>.

<sup>(68)</sup> Datos disponibles en el Observatorio de Administración Electrónica. Accesible en: <http://dataobsae.administracionelectronica.gob.es/> (última consulta: mayo de 2017).

El intercambio electrónico de datos tiene una repercusión directa en la protección de datos personales en la medida en que constituye una cesión o comunicación de datos, es decir, una revelación de datos realizada a una persona distinta del interesado<sup>69</sup>. Al respecto, debemos recordar que los datos personales únicamente pueden ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del

<sup>(69)</sup> Artículo 3.1.d) LOPD.

cesionario, con el previo consentimiento del interesado. La propia LOPD prevé algunas particularidades en el caso de la comunicación de datos personales entre Administraciones públicas respecto a lo previsto con carácter general:

«Los datos de carácter personal objeto del tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado»<sup>70</sup>.

<sup>(70)</sup>Artículo 11 LOPD.

En efecto, el artículo 21 LOPD establece un régimen específico para la comunicación o cesión de datos entre Administraciones públicas que se caracteriza por prever diferentes supuestos en los que no será necesario el consentimiento del afectado para poder comunicar datos personales entre Administraciones públicas.

«1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos».

A la vista de lo anterior, deben tenerse en cuenta los elementos siguientes:

### 1) **Ámbito subjetivo**

Según el artículo 2 LRJSP, tienen la consideración de Administración pública la Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración local, así como los organismos públicos y las entidades de derecho público vinculados o dependientes de las Administraciones públicas<sup>71</sup>.

<sup>(71)</sup>En el mismo sentido, el artículo 2.3 LPACAP.

### 2) **Ámbito objetivo**

La Administración pública cedente debe cumplir con los requisitos previstos en la LOPD por lo que se refiere al tratamiento de los datos. En el caso de los datos recogidos por una Administración pública con destino a otra, estos no estarán vinculados a las atribuciones de la Administración pública que comunique los datos, sino de la Administración pública que los deba recibir.

### 3) **Tratamientos incluidos**

a) Datos para el ejercicio de las mismas competencias o las competencias que versen sobre las mismas materias para los que fueron recogidos. No será necesario el consentimiento del afectado si los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones son comunicados a otras Administraciones públicas para el ejercicio

de las mismas competencias o las competencias que versen sobre las mismas materias. Al respecto, se puede traer a colación la sentencia del Tribunal Supremo de 15 de abril de 2002, en la que se reconoce que

«la cesión o comunicación de los datos entre Administraciones públicas, mientras se lleve a cabo, precisa y únicamente, para alcanzar el fin o uno de los fines a los que obedece la creación misma del fichero y la propia recogida de aquellos, y no, por tanto, para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, queda ya amparada por el consentimiento inicialmente prestado por el titular de los datos para su recogida y tratamiento. Es decir, en tal caso, huelga la necesidad de un nuevo consentimiento cuyo objeto específico sea aquella cesión o comunicación»<sup>72</sup>.

(72) RJ\2002\4689.

b) Datos con fines históricos, estadísticos o científicos.

c) Datos obtenidos o elaborados con destino a otra.

d) Otros supuestos de comunicación de datos entre Administraciones públicas previstos en otras normas:

- **Datos de la Administración tributaria.** No será de aplicación lo previsto en el artículo 21.1 LOPD cuando la cesión de datos de carácter personal que se deba efectuar a la Administración tributaria, conforme a lo dispuesto en el artículo anterior, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado<sup>73</sup>.
- **Padrón municipal de habitantes.** Otro caso con amplias repercusiones se encuentra en relación con el padrón municipal de habitantes. La Ley orgánica 14/2003, de 20 de noviembre, incluyó en la LBRL algunos cambios con el fin de facilitar la cesión de datos del padrón municipal de habitantes. En particular, en la actualidad el artículo 16.3 LBRL prevé que los datos del padrón municipal se cederán a otras Administraciones públicas que lo soliciten sin consentimiento previo al afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias y, exclusivamente, para asuntos en los que la residencia o el domicilio sean datos relevantes<sup>74</sup>.

(73) Artículo 94.5 Ley 58/2003, de 17 de diciembre, general tributaria.

(74) Así lo ha confirmado, por ejemplo, la Sentencia del Tribunal Superior de Justicia de Cataluña, Sala de lo Contencioso-administrativo, Sección 5.ª, de 19 de diciembre de 2006.

Las Administraciones públicas deberían facilitar información al ciudadano sobre las cesiones de datos entre Administraciones públicas especialmente cuando las cesiones se realizan sin su consentimiento a pesar de que no está explícitamente previsto<sup>75</sup>. En cualquier caso, aunque se puede considerar que la presentación de la solicitud por el interesado puede considerarse como una

(75) En esta dirección, el grupo del artículo 29 en su informe sobre la administración electrónica.

autorización tácita para que la Administración pública pueda acceder a los datos necesarios para su tramitación, ello no es obstáculo para que las solicitudes incorporen explícitamente dicho consentimiento.

De hecho, a pesar de que no esté explícitamente previsto, sería deseable el hecho de informar al interesado sobre las cesiones de datos entre Administraciones públicas, especialmente cuando se realizan sin su consentimiento<sup>76</sup>.

### Informar previamente

En esta dirección se pronuncia la Sentencia del Tribunal de Justicia de la Unión Europea de 1 de octubre de 2015 (Asunto C-201/14), donde se declara que las personas cuyos datos personales son objeto de transmisión y tratamiento entre Administraciones públicas deben ser informadas de ello previamente. En particular, tal y como se manifiesta en el fundamento jurídico 34 de dicha Sentencia, «la exigencia de tratamiento leal de los datos personales prevista en el artículo 6 de la Directiva 95/46 obliga a una Administración pública a informar a los interesados de la transmisión de esos datos a otra Administración pública para su tratamiento por esta en su calidad de destinataria de dichos datos».

El intercambio de documentos electrónicos entre Administraciones públicas, en entornos cerrados de comunicaciones, garantiza la autenticación y la identificación de los emisores y los receptores, y también puede garantizar la integridad de los documentos intercambiados<sup>77</sup>.

Las condiciones y garantías que se establezcan deberán darse tanto para poder acceder al entorno cerrado como para la transmisión de datos, y deberán garantizar la seguridad del entorno cerrado de comunicación y la protección de los datos personales que se transmitan. En esta dirección, es necesario tener presentes las características previstas por el Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad.

Cuando los emisores y receptores de los documentos electrónicos pertenezcan a una misma Administración pública, será esta la que concrete las condiciones y garantías por las que se registrará el intercambio de documentos en el entorno cerrado. Estas condiciones deberán concretar la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar. Cuando los emisores y receptores pertenezcan a distintas Administraciones públicas, las condiciones y garantías deberán establecerse mediante convenio suscrito entre ellas<sup>78</sup>.

### Normas para el intercambio electrónico de datos

Los proyectos para el intercambio electrónico de datos han encontrado acomodo en diferentes normas. Así, se puede traer a colación lo previsto en el Decreto 56/2009, de 7 de abril, para el impulso y el desarrollo de los medios electrónicos en la Administración. La Generalitat de Cataluña ha formalizado el Catálogo de datos y documentos electrónicos, que es la relación actualizada de datos y documentos que se encuentran en poder de los entes y órganos de la Administración de la Generalitat de Cataluña y de otras administraciones e instituciones públicas que se pueden obtener por medios electrónicos para hacer efectivo el derecho de los ciudadanos a no aportar documentos. Según el artículo 18, la inclusión de un dato o documento en dicho Catálogo implica que no se podrá pedir a los ciudadanos. De todos modos, no se puede desconocer que «este derecho está

#### Autorización tácita para la Administración pública

En esta línea, el artículo 28.3 Ley 38/2003, de 17 de noviembre, general de subvenciones establece que «la presentación de la solicitud por parte del beneficiario conllevará la autorización al órgano gestor para recabar los certificados a emitir por la Agencia Estatal de Administración Tributaria y por la Tesorería General de la Seguridad Social» (Valero Torrijos, 2010, pág. 277).

<sup>(76)</sup> Informe del Grupo de Trabajo sobre Protección de Datos del Artículo 29 sobre administración electrónica de 8 de mayo de 2003 (10593/02/ES WP 73). Asimismo: Troncoso Reigada, 2008, pág. 79.

<sup>(77)</sup> Artículo 44.1 LRJSP.

<sup>(78)</sup> Artículo 44.2 y 3 LRJSP.

#### Art. 21 Ley 29/2010

Véase, asimismo, el artículo 21 Ley 29/2010, de 3 de agosto, de uso de los medios electrónicos por el sector público de Cataluña, que prevé la creación del Catálogo de datos y documentos interoperables de Cataluña que es la herramienta de que se dota el sector público de Cataluña para hacer efectivo el derecho de los ciudadanos a no aportar datos y documentos que están en poder de las Administraciones públicas. El Catálogo es gestionado por el consorcio Administración Oberta de Catalunya.

condicionado a la prestación, si procede, del consentimiento de la persona interesada a la entidad que requiere estos datos y documentos, de acuerdo con lo que prevé la normativa de protección de datos».



## Abreviaturas

**LOPD** Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

**LPACAP** Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones públicas.

**LRISP** Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

**LRJSP** Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

**LTAIGB** Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

**RGPD** 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).

## Bibliografía

**Cerrillo Martínez, A.** (2010a). «Cooperación entre Administraciones públicas para el impulso de la Administración electrónica». En: E. Gamero Casado; J. Valero Torrijos (eds.). *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* (3.ª ed.). Cizur Menor: Thomson-Aranzadi.

**Cerrillo Martínez, A.** (2010b, enero-abril). «La administración electrónica en el derecho autonómico comparado». *Revista Vasca de Administración Pública. Herri-Ardularitzako Euskal Aldizkaria* (núm. 86, págs. 15-60).

**Cerrillo Martínez, A.** (ed.) (2016). *A las puertas de la administración digital. Una guía detallada para la aplicación de las Leyes 39/2015 y 40/2015*. Madrid: Instituto Nacional de Administración Pública.

**Cerrillo Martínez, A.; Casadesús, A.** (2016). *La transparencia por diseño: el impacto de la gestión documental en la transparencia pública*.

**Cerrillo Martínez, A.; Galán Galán, A.** (2007). *Qualitat i responsabilitat en la difusió d'informació pública a Internet*. Barcelona: Escola d'Administració Pública de Catalunya i Generalitat de Catalunya.

**Comisión Europea** (2011). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre Datos abiertos. Un motor para la innovación, el crecimiento y la gobernanza transparente - COM(2011) 882 final*.

**Cotino Hueso, L.** (2013). «Derecho y “Gobierno Abierto”. La regulación de la transparencia y la participación y su ejercicio a través del uso de las nuevas tecnologías y las redes sociales por las Administraciones públicas. Propuestas concretas». *Monografías de la Revista Aragonesa de Administración Pública* (núm. XIV, págs. 51-92).

**Fernández Ramos, S.; Pérez Monguió, J. M.** (2017). *El Derecho de acceso a la información pública en España*. Cizur Menor: Thomson-Reuters-Aranzadi.

**Fernández Salmerón, M.** (2003). *La protección de los datos personales en las Administraciones públicas*. Madrid: Civitas / Agencia de Protección de Datos de la Comunidad de Madrid.

**Grupo de Trabajo sobre Protección de Datos del Artículo 29.** (2003). *Documento de trabajo sobre la administración en línea*.

**Grupo de Trabajo sobre Protección de Datos del Artículo 29.** (2014). *Dictamen 05/2014 sobre técnicas de anonimización*.

**Guichot Reina, E.** (2005). «Derecho a la protección de datos y actividad administrativa». *Revista Vasca de Administración Pública* (núm. 71, págs. 81-120).

**Troncoso Reigada, A.** (2008). «La administración electrónica y la protección de datos personales». *Revista Jurídica de Castilla y León* (núm. 16).

**Valero Torrijos, J.** (2010). «Acceso a los servicios y a la información por medios electrónicos». En: E. Gamero Casado; J. Valero Torrijos (eds.). *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* (3.ª ed.). Cizur Menor: Thomson-Aranzadi.

**Valero Torrijos, J.** (2012). «La Ley 11/2007 cinco años después balance desde la perspectiva jurídica». *Bole.tic* (núm. 63).