CAPÍTULO IV

LA ADMINISTRACIÓN ELECTRÓNICA Y LA PROTECCIÓN DE DATOS PERSONALES(1)

ANTONIO TRONCOSO REIGADA

Profesor Titular de Derecho Constitucional
Director de la APDCM 2002-2009

SUMARIO: I. PLANTEAMIENTO GENERAL. *1. El significado constitucional de la modernización administrativa y la legitimidad de la Administración Pública. 2. La Administración electrónica: nuevos derechos y nuevos riesgos.* II. LA PROTECCIÓN DE DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA. *1. El incremento de los tratamientos de datos personales en la Administración electrónica. 2. La protección de datos personales como oportunidad para la Administración electrónica. 3. Las tecnologías de protección del derecho a la intimidad y la privacy by design. 4. La declaración de ficheros y tratamientos de datos personales en la Administración electrónica y la función del responsable.* III. EL PRINCIPIO DE CALIDAD EN LA ADMINISTRACIÓN ELECTRÓNICA. *1. El principio de finalidad y el acceso por los Departamentos de la misma Administración. 2. El principio de adecuación y prohibición de exceso. 3. El principio de exactitud y la actualización de la información. 4. La cancelación de la información. 5. El DNI electrónico: finalidad y datos objeto de tratamiento.* IV. LA INFORMACIÓN Y EL CONSENTIMIENTO PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA. *1. La información al interesado de los distintos tratamientos (accesos, cesiones individualizadas, interconexiones, comprobaciones automatizadas, verificación de la autenticidad de la información). 2. El consentimiento del interesado para el tratamiento de sus datos en los servicios de Administración electrónica para el cumplimiento de funciones administrativas y para actividades complementarias (servicios de noticias y alertas y uso de «cookies»).* V. LAS COMUNICACIONES DE DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA. *1. El consentimiento del interesado y la habilitación legal. 2. Tres supuestos de consentimiento tácito: el derecho a no aportar datos y documentos que obren en poder de las Administraciones Públicas; las comprobaciones de las copias digitales de los documentos aportados por los ciudadanos y la verificación de la autenticidad de los datos personales contenidos en las solicitudes que se dirigen a la Administración. La problemática del formulario previamente cumplimentado. 3. Otros supuestos que legitiman la comunicación de datos personales entre Administraciones Públicas. 4. Los accesos automatizados, las interconexiones de bases de datos y el respeto a los principios de calidad y de proporcionalidad.* VI. LA SEGURIDAD DE LA INFORMACIÓN COMO GARANTÍA DE LA INTEGRIDAD, AUTENTICIDAD Y CONFIDENCIALIDAD EN LA ADMINISTRACIÓN ELECTRÓNICA. VII. EL EJERCICIO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN ELECTRÓNICA Y LAS COMPETENCIAS DE LAS AUTORIDADES DE CONTROL.

---

(1) Una primera aproximación a esta cuestión ha sido realizada en la *Revista Jurídica de Castilla y León*, nº 16, 2008, pp. 31-111. Estas páginas suponen una revisión sustancial de ese texto.

I. PLANTEAMIENTO GENERAL

1. EL SIGNIFICADO CONSTITUCIONAL DE LA MODERNIZACIÓN ADMINISTRATIVA Y LA LEGITIMIDAD DE LA ADMINISTRACIÓN PÚBLICA

La introducción de las nuevas tecnologías en la Administración Pública no es un fin en sí mismo sino que tiene que comprenderse y analizarse como un instrumento de cambio y de modernización administrativa que permite a la Administración ser más eficaz en el servicio al interés general y en la promoción de los derechos fundamentales. Los proyectos de gobierno electrónico se enmarcan, de esta manera, dentro de las iniciativas que tratan de mejorar la calidad de los servicios públicos, contribuyendo a acercar la Administración a los ciudadanos y, en definitiva, a mejorar la satisfacción de éstos por los servicios públicos que reciben(2).

Las nuevas tecnologías facilitan un nuevo cauce de relación entre la Administración y los ciudadanos, de manera que ésta no sea sólo presencial, sino también telefónica o a través de Internet. De esta forma, la relación ciudadano-administración se vuelve más cómoda y más sencilla,

---

(2) Hemos analizado en otro momento las nuevas tecnologías como instrumento de modernización de las Administraciones Públicas. Cfr. A. TRONCOSO REIGADA, «Las Cartas de Servicio: un compromiso con el ciudadano», *La Mejora de la Calidad*, Gobierno de La Rioja, Logroño, 2004, pp. 97-108 y «La Administración electrónica y la protección de datos personales», en *Revista Jurídica de Castilla y León*, cit., pp. 35-41. Cfr. especialmente J. L. PIÑAR MAÑAS, «Revolución tecnológica, Derecho administrativo y Administración Pública. Notas provisionales para una reflexión» en T. R. FERNÁNDEZ y otros, *La Autorización administrativa. La Administración Electrónica. La enseñanza del Derecho Administrativo hoy*, Aranzadi, Cizur Menor, 2007, pp. 51-92; J. BARNÉS VÁZQUEZ, «Una reflexión introductoria sobre Derecho Administrativo y la Administración Pública de la Sociedad de la Información y el Conocimiento», *Revista Andaluza de Administración Pública*, nº 40, 2000; J. FERNÁNDEZ RODRÍGUEZ, *Gobierno Electrónico. Un desafío en Internet*, FUNDAP, 2004; *Libro Blanco para la Mejora de los Servicios Públicos*: *Una nueva Administración al servicio de los ciudadanos*, MAP, 2000. La Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones, titulada «El papel de la administración electrónica en el futuro de Europa» –de 26 de septiembre de 2003–, –COM (2003) 567 final–, señala que «[l]as tecnologías de la información y las comunicaciones pueden ayudar a las Administraciones Públicas a hacer frente a tantos retos. Sin embargo, el énfasis no 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. A eso se refiere la Administración electrónica *(eGovernment)*». En este marco se encuadran la aprobación de Cartas de Servicio –manifestación visible de la voluntad de la Administración por mejorar la calidad del servicio que presta e instrumento con que cuentan los ciudadanos para facilitar el ejercicio de sus derechos cívicos–, los Premios a la Excelencia y Calidad de los Servicios Públicos o los sistemas de sugerencias y reclamaciones. Muestra de ello es que el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, establece que las sedes electrónicas dispondrán de carta de servicios electrónicos y de un enlace para la formulación de sugerencias y quejas –art. 6.2–.

al poder desarrollarse a todas las horas y desde el propio domicilio o lugar de trabajo(3). Además, las nuevas tecnologías no sirven sólo para mejorar la información que las Administraciones Públicas dan a los ciudadanos sino también para permitir la tramitación electrónica de los procedimientos administrativos. Es decir, es importante no sólo que se pueda acceder de manera electrónica a la información de los principales servicios sino que el ciudadano pueda presentar su solicitud cómodamente desde el ordenador, para pedir, por ejemplo, una subvención, matricularse en una Universidad, pedir cita en un centro de salud o conocer el estado de tramitación de un expediente administrativo.

La Administración electrónica y la progresiva introducción de las nuevas tecnologías no sólo conllevan un cambio en la relación con los ciudadanos sino también en la propia cultura interna de la Administración. Así, la voluntad de ofrecer Internet como canal para relacionarse con la Administración obliga no sólo a la automatización del *back office* administrativo y a la mecanización de los procedimientos sino también a su previo rediseño, a través de un diagrama de flujos y procesos, de forma que la gestión administrativa se haga más rápida y más clara para los ciudadanos. De esta forma, la Administración electrónica lleva aparejada el impulso a los procesos de simplificación administrativa(4). Esto signi-

(3) Como señala la Exposición de Motivos de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos –LAECSP–, la Administración electrónica permite superar «la barrera que sigue distanciando todavía al ciudadano de la Administración, de cualquier Administración, incluida la del Estado, y que muchas veces no es otra que la barrera que levanta el tiempo y el espacio: el tiempo que hay que dedicar a la relación con aquélla para la realización de muchos trámites de la vida diaria que empiezan a veces por la necesidad de una primera información que exige un desplazamiento inicial, más los sucesivos desplazamientos y tiempo que se dedican a posteriores trámites a hacer con la Administración para las actividades más elementales. […] Las tecnologías de la información y las comunicaciones hacen posible acercar la Administración hasta la sala de estar de los ciudadanos o hasta las oficinas y despachos de las empresas y profesionales. Les permiten relacionarse con ella sin colas ni esperas. […]. Pero, además de eso, las nuevas tecnologías de la información facilitan, sobre todo, el acceso a los servicios públicos a aquellas personas que antes tenían grandes dificultades para llegar a las oficinas públicas, por motivos de localización geográfica, de condiciones físicas de movilidad u otros condicionantes, y que ahora se pueden superar por el empleo de las nuevas tecnologías» –apdo. I–. Así, el Real Decreto 1671/2009, de 6 de noviembre, establece que la presentación de solicitudes, escritos y comunicaciones podrá realizarse en los registros electrónicos durante las veinticuatro horas de todos los días del año, pudiendo únicamente interrumpirse por el tiempo imprescindible sólo cuando concurran razones justificadas de mantenimiento técnico u operativo –art. 30–.

(4) Los primeros trabajos en esta dirección se hicieron en los años noventa. Cfr. *Guía para el rediseño de procedimientos administrativos de la Comunidad de Madrid*, Comunidad de Madrid, 1998; *Gestiona tú mismo. Plan Estratégico de Simplificación de la Gestión Administrativa. Administración electrónica*. Comunidad de Madrid, 2002; J. BALDERSTON, *Cómo organizar y simplificar el trabajo administrativo*, Deusto, 1993; *Técnicas de simplificación del trabajo administrativo. La elaboración de manuales de procedimientos*; MAP, 1999. Quisiera destacar el Anteproyecto de Ley de la Comunidad de Madrid de Medidas de Simplificación y Racionalización administrativa que reformaba la legislación autonómica, de Gobierno y Administración, de subvenciones de hacienda, de la función pública y del patrimonio, elaborado en el año 2000

fica suprimir trámites redundantes o innecesarios, reducir la documentación que se exige a los ciudadanos –especialmente aquellos documentos que ya tenga la Administración y que se pueden obtener a través de la interconexión de registros administrativos–, implantar bases generales de procedimientos y plazos únicos y la instauración progresiva del silencio positivo como regla general. Todo ello permite una gestión administrativa más rápida y más clara para los ciudadanos.

La Administración electrónica también mejora la participación de los usuarios en el diseño y gestión de los servicios públicos. De hecho, el incremento de la satisfacción de los ciudadanos por los servicios que reciben pasa principalmente por escuchar a los usuarios. De los distintos servicios que puede prestar una Administración y de las distintas alternativas para desarrollar un servicio, la que aprovecha mejor los fondos públicos es siempre aquella que desean los ciudadanos. Es imprescindible preguntar a los ciudadanos para determinar qué servicios son los que más valoran, los que más necesitan, de manera que se puedan organizar estos servicios en función de sus necesidades. Dentro de este esfuerzo por fomentar la participación, hay que resaltar que Internet es una buena herramienta para tomar en consideración la opinión de los ciudadanos sobre los servicios que presta la Administración, para recibir sus sugerencias y reclamaciones y, en definitiva, para desarrollar una atención al ciudadano de calidad. La participación ciudadana es la clave para la mejora de los servicios públicos y las nuevas tecnologías facilitan esta participación(5).

---

durante mi etapa como Director General de Calidad de los Servicios en el Gobierno de Ruiz Gallardón, cuyos preceptos fueron después incluidos en la Ley de Acompañamiento a los Presupuestos de 2001. También en esta etapa se aprobaron setenta y dos Cartas de Servicio.

(5) La web 2.0 facilita mucho esta participación. Estamos hablando de que las nuevas tecnologías faciliten la participación social, pero no estamos abordando ahora la problemática de la participación política a través de las nuevas tecnologías. Hay que diferenciar la participación de los ciudadanos en la toma de decisiones de gestión, escuchando a los usuarios de los servicios públicos a través de Internet, de la participación política, que sirve para conformar la voluntad general, que también se puede ejercitar por medios electrónicos, a través de lo que se ha denominado democracia electrónica y voto electrónico. Esta última plantea muchos más problemas que abordaremos posteriormente. Cfr. L. COTINO HUESO, «De qué hablamos cuando hablamos de democracia y participación electrónicas», en AA VV, *Cuestiones Actuales de Derecho de las Tecnologías de la Información y Comunicación*, Thomson-Aranzadi, Cizur Menor, pp. 43-62; y L. COTINO HUESO (coord.) *Libertades, democracia y gobierno electrónicos*, Comares, Granada, 2005. En todo caso, ha habido buenas experiencias de debate de anteproyectos de ley a través de Internet, como se hizo con la ley de firma electrónica. El Ayuntamiento de Madrid ha planteado distintas iniciativas de participación social a través de medios electrónicos –la iniciativa «Madrid Participa»– que se encuentran recogidas en el documento *Democracia electrónica y participación ciudadana. Informe tecnológico y funcional sobre la Consulta Ciudadana*, Madrid, Participa, julio 2004. Recientemente se ha tratado de introducir el voto electrónico en las Juntas Generales de Accionistas, siguiendo la recomendación de la Ley de Transparencia para facilitar por todos los medios posibles el voto a distancia, lo que ha llevado a la modificación de muchos Estatutos. Así, más de la mitad de las empresas del IBEX 35 tiene canales electrónicos aunque los accionistas prefie-

La Administración electrónica también permite –frente a la Administración tradicional– un ahorro de los recursos públicos, lo que aporta enormes ventajas en términos de eficiencia. La necesidad de incrementar –o al menos mantener– el gasto en las partidas más marcadamente sociales como la educación, la sanidad o los servicios sociales obliga a replantear el gasto corriente que representa todavía un porcentaje elevado de los presupuestos públicos(6). La mejora de la calidad de los servicios públicos en un contexto de crisis económica puede venir de la mano del ahorro de recursos que supone la Administración electrónica(7). Así, por ejemplo, la documentación electrónica facilita su localización y evita la pérdida de esfuerzos y tiempo que supone la acumulación de información en papel(8). La informatización y la automatización de procedimientos reducen asimismo las necesidades de personal administrativo. En general, la introducción de las nuevas tecnologías en la Administración Pública permite la eficiencia en el uso de los fondos públicos que tienen su origen y que deben tener su destino en la sociedad.

La Administración electrónica también facilita el intercambio de conocimiento dentro de la Administración Pública. La mejora de los servicios públicos es una labor continua y una labor de todos. No estamos hablando únicamente de cómo las nuevas tecnologías permiten la formación virtual del personal al que no alcanza la formación presencial. Nos referimos a cómo las nuevas tecnologías favorecen la gestión del conocimiento en las Administraciones Públicas. Una Administración con tantos empleados públicos es rica en experiencias de buenas prácticas que deben ser trasladadas a otras unidades. Todo servicio público está basado en el conocimiento, que es el auténtico motor del proceso de mejora en la Administración Pública. La Administración no tiene dinero pero sí

---

ren todavía el correo postal a la hora de remitir sus votos a distancia. Cfr. *Cinco días*, jueves, cuatro de agosto de 2005.

(6) Una buena muestra de cómo la introducción de las nuevas tecnologías supone una reducción del gasto corriente es el ámbito sanitario donde proyectos como la receta electrónica, la historia clínica electrónica, la utilización de las tecnologías para el almacenamiento de pruebas diagnósticas o la telemedicina, además de suponer una mejora de la calidad asistencial, permiten la reducción del coste de la asistencia y del tiempo que el personal facultativo emplea en localizar la información. Cfr. nuestra «Introducción y Presentación» a *Protección de datos personales para Servicios Sanitarios Públicos*, Civitas-APDCM, Madrid, 2008, pp. 11-15.

(7) No obstante, llama la atención que el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, no incide en que el acceso electrónico de los ciudadanos a los servicios públicos supone un ahorro sino que se limita a señalar que «la aplicación de las previsiones contenidas en este Real Decreto no deberá ocasionar incremento del gasto público ni disminución de los ingresos públicos. Por tanto, los departamentos ministeriales afectados deberán desarrollar las medidas derivadas de su cumplimiento ateniéndose a sus disponibilidades presupuestarias ordinarias, no dando lugar, en ningún caso, a planteamientos de necesidades adicionales de financiación» –Disposición Adicional Sexta–.

(8) Cfr. *La informática en las Administraciones Públicas. Informe IRIA-94*, MAP, 1995; *Las Tecnologías de la Información en las Administraciones Públicas. Informe IRIA*, MAP, 2001.

talento humano que es lo que marca la diferencia. La gestión del conocimiento cobra, de esta forma, un papel indispensable en el aprovechamiento e intercambio de los proyectos de mejora y en el aprendizaje mutuo entre las distintas Administraciones Públicas. Las tecnologías de la información –especialmente Internet– facilitan la creación de redes de *benchmarking* y favorecen la gestión del conocimiento y de las mejores prácticas(9).

Por tanto, la implantación de las nuevas tecnologías contribuye a mejorar la actividad administrativa en beneficio del interés general y a actuar de conformidad con el principio de eficacia, lo que fortalece la legitimidad de la Administración Pública. Si bien la Administración Pública tiene una legitimidad jurídica –que proviene de la aplicación objetiva de la norma que refleja la voluntad general– y una legitimidad política –porque es dirigida por un gobierno que está sometido a controles políticos en aplicación del principio democrático–, también los poderes públicos deben buscar la legitimidad social que se alcanza con la calidad de los servicios públicos, con la satisfacción de los usuarios y con el respeto al principio de eficacia(10). Además, el desarrollo de la Administración electrónica permite dar una información administrativa más extensa sobre concursos, contratos, subvenciones, procesos selectivos, no sólo a ciudadanos en concreto sino a asociaciones y a la sociedad en general; una información que, en ocasiones, sólo tenían funcionarios y grupos de interés. De esta forma, la Administración electrónica mejora la posición de los ciudadanos frente a la Administración Pública e incrementa la transparencia administrativa y el control social sobre la misma(11), una

(9) HEGEL señalaba que el conocimiento es, sobre todo, un proceso y que, además, es progresivo: La razón –el espíritu universal– es algo dinámico y transcurre dentro de un proceso. Cfr. sobre la importancia de la gestión del conocimiento en la Administración Pública nuestra «Introducción» a la *Memoria del I Premio Europeo de Mejores Prácticas de las Administraciones Públicas en Protección de Datos Personales*, Civitas, Madrid, 2005.

(10) Cfr. L. PAREJO ALFONSO, *Eficacia y Administración. Tres estudios*, INAP, 1995. Cfr. también A. VALARIE, A. ZEITHAML, L. BERRY, *Calidad total en la gestión de servicios*. Delivering Quality Service, Díaz de Santos, 1992; *Evaluando servicios y políticas públicas*, Gobierno de Cantabria, Consejería Presidencia, 2006; *Gestión y Evaluación de la Calidad en los Servicios Públicos*. Segundas Jornadas sobre Medición y Mejora de los Servicios Públicos; MAP, 1995.

(11) A través de nuevas tecnologías de la comunicación los ciudadanos pueden estar mejor informados de los servicios que presta y que pueden ser exigidos a una Administración Pública, así como de los procedimientos selectivos o de subvenciones. Piénsese, por ejemplo, en un proceso selectivo que, previo establecimiento en las bases de la convocatoria, permite un mayor conocimiento del resultado de cada una de las pruebas a través de su publicación en una página web accesible a los interesados. Esto lógicamente favorece la capacidad de control. Así, se ha afirmado que los peligros que pudieran venir derivados de una mayor capacidad por parte de la Administración Pública en el tratamiento de la información personal pueden verse compensados con un mayor control externo de tales actuaciones que garantice, a la vez que la eficacia, la legalidad de las mismas. Cfr. P. GARCÍA-POGGIO, «Hacia una nueva Administración Pública en la Sociedad de la Información», *Actualidad Informática Aranzadi*, nº 32, 1999, p. 8.

cuestión que hemos abordado en otro momento al analizar los fundamentos constitucionales del acceso a información administrativa(12).

Además, el desarrollo de la Administración electrónica, como señaló la Comisión Soto, es una de las medidas fundamentales para el progreso de la sociedad de la información, un área vertical y de prioridad fundamental debido al factor de arrastre y al liderazgo que la Administración Pública puede tener sobre el sector privado y sobre la sociedad en general. La puesta *on line* de servicios públicos prestados tradicionalmente a través de una ventanilla física supone un incentivo para que los ciudadanos accedan a la sociedad de la información. De esta forma, la Administración electrónica no es sólo una oportunidad histórica para avanzar hacia un mejor gobierno del Estado, aumentando la eficiencia y ofreciendo un mejor servicio al ciudadano. También la Administración electrónica y la integración de las tecnologías de la información en los servicios públicos es un factor fundamental para el desarrollo de la sociedad de la información, también en el ámbito privado y de las relaciones comerciales.

2. LA ADMINISTRACIÓN ELECTRÓNICA: NUEVOS DERECHOS Y NUEVOS RIESGOS

Hemos analizado en otro momento cómo se pasa de la teoría de la Administración electrónica a la realidad(13) y cuáles han sido las iniciativas y los obstáculos que se han encontrado en el camino entre la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común –que ya regula la utilización de las técnicas electrónicas, informáticas y telemáticas a la actividad administrativa y a las relaciones de los ciudadanos con las Administraciones Públicas, asumiendo que la adaptación a las nuevas tecnologías debía ser una característica permanente de las Administraciones Públicas

(12) Cfr. nuestro trabajo «Transparencia administrativa y protección de datos personales», en A. TRONCOSO REIGADA, *Transparencia administrativa y protección de datos personales*, Civitas-APDCM, Madrid, 2008, pp. 23-188.

(13) Nos remitimos a la exposición histórica que hemos hecho en «La Administración electrónica y la protección de datos personales», cit., pp. 41-59. Cfr. como referencia general J. VALERO TORRIJOS, *El régimen jurídico de la e-Administración*, Comares, Granada, 2004. Cfr. también E. GAMERO CASADO, «El Derecho administrativo en la era de la información», en E. GAMERO CASADO y J. VALERO TORRIJOS (Coord.), *La Ley de Administración Electrónica*, Thomson-Aranzadi, Cizur Menor, 2008, pp. 29-56. Hay que recordar que ya la Ley de Procedimiento Administrativo de 1958 dedicó algunos preceptos «a la normalización de documentos, a la racionalización, mecanización y automatización de los trabajos en las oficinas públicas, a la creación de Oficinas de Información y de Reclamaciones y a la fijación de horarios adecuados para el mejor servicio de los administrados». Cfr. A. SÁNCHEZ NAVARRO, «La articulación del derecho a la protección de datos de carácter personal en la gestión electrónica de los procedimientos administrativos», *Revista Española de Protección de Datos* , nº 3, 2007, p. 103.

españolas(14)– y la nueva Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos –LAECSP–(15).

La LAECSP reconoce el derecho de todos «a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el art. 35 de la LRJAP y PAC, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos» –art. 6.1 LAECSP–(16). Se trata no sólo de que las Administraciones puedan ofrecer servicios, sino que los ciudadanos tengan el derecho de exigirlos y puedan hacer sus trámites a través de la red(17). Como

(14) En este período hay que destacar especialmente la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, que modifica varios artículos de la Ley 30/1992, de 26 de noviembre, la Ley 58/2003, de 17 de diciembre, General Tributaria, que recoge por primera vez la automatización de la actuación administrativa o la obtención de imágenes electrónicas de los documentos con idéntica validez y eficacia que el documento origen, la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, que establece el DNI electrónico, la Ley 56/2007, de 28 de diciembre de Medidas de Impulso de la Sociedad de la Información, que introduce previsiones específicas de impulso de la factura electrónica y del uso de medios electrónicos en todas las fases de los procesos de contratación. Durante estos años, el Gobierno también ha desarrollado un conjunto de medidas enfocadas a facilitar la Administración Electrónica. Así, el Consejo de Ministros aprobó los Reales Decretos 522/2006 y 523/2006, de 28 de abril, por los que se suprime la aportación de fotocopias del documento nacional de identidad o del certificado de empadronamiento por parte de los interesados en los procedimientos administrativos tramitados por la Administración General del Estado y de sus organismos públicos vinculados o dependientes.

(15) El planteamiento de la Unión Europea para la promoción de la sociedad de la información se denominó e-Europe. Su primera edición (e-Europe 2002) se aprobó por el Consejo Europeo de Lisboa –marzo de 2000–, y la segunda (que se llama e-Europe 2005) por el Consejo Europeo de Sevilla –junio de 2002–. Se realizó una revisión de resultados de e-Europe 2005, cuyo resumen está disponible en *http://europa.eu.int/information_society/eeurope/2005/doc/all_about/acte_en_version_finale.pdf*. Cfr. también el informe *Online Availability of Public Services: How is Europe Progressing?*, en *http://europa.eu.int/information_society/eeurope/i2010/docs/benchmarking/online_availability_2006.pdf* . Hay que destacar también el Programa IDA *(Interchange of Data between Administrations)*, que se inició a partir de la Decisión 95/468/CE, orientado al intercambio de información entre las Administraciones de los países europeos y las instituciones comunitarias. Con posterioridad las Decisiones 1719/1999/CE y 1720/1999/CE pusieron en marcha el programa IDA II, orientado a la prestación de servicios públicos en línea a ciudadanos y empresas. Posteriormente se aprobó la Decisión 2004/387/CE que pone en marcha la iniciativa IDABC *(Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens)* que era una continuación de los anteriores.

(16) Cfr. E. Gamero Casado y J. Valero Torrijos (Coord.), *La Ley de Administración Electrónica. Comentario sistemática a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, Thomson-Aranzadi, Cizur Menor, 2008.

(17) El art. 45.2 LRJ-PAC se limitaba a señalar que «[c]uando 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 con respecto de las garantías y requisitos previstos en cada procedimiento». Como señala la Exposición de Motivos de la LAECSP este precepto «deja[n] en manos de las propias Administraciones determinar si los ciu-

señala la Exposición de Motivos, «[e]l servicio al ciudadano exige consagrar su derecho a comunicarse con las Administraciones por medios electrónicos. La contrapartida de ese derecho es la obligación de éstas de dotarse de los medios y sistemas electrónicos para que ese derecho pueda ejercerse. Ésa es una de las grandes novedades de la Ley: pasar de la declaración de impulso de los medios electrónicos e informáticos –que se concretan en la práctica en la simple posibilidad de que algunas Administraciones, o algunos de sus órganos, permitan las comunicaciones por medios electrónicos– a que estén obligadas a hacerlo porque la Ley reconoce el derecho de los ciudadanos a establecer relaciones electrónicas»(18). El derecho a utilizar los medios de comunicación electrónica para relacionarse con la Administración implica, como ha señalado la Exposición de Motivos del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, considerar al ciudadano como portador de un derecho de prestación que la Administración debe satisfacer de forma efectiva. Esta Ley establece el plazo del 31 de diciembre de 2009 para que las Administraciones Públicas permitan el acceso electrónico de los ciudadanos a todos sus procedimientos administrativos(19), lo que también se aplica a las Agencias de

---

dadanos van a poder de modo efectivo o no, relacionarse por medios electrónicos con ellas, según que éstas 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» –apdo. I–. Cfr. L. COTINO HUESO, «Los derechos del ciudadano», E. GAMERO CASADO y J. VALERO TORRIJOS (Coord.), *La Ley de Administración Electrónica*, cit., pp. 119-225 –especialmente en relación con la dimensión prestacional del derecho a relacionarse por medios electrónicos, pp. 157-165–.

(18) La Exposición de Motivos de esta Ley señala que ésta es una respuesta a los compromisos comunitarios y a las iniciativas europeas a partir del Consejo Europeo de Lisboa y de Santa María da Feira hasta la actual comunicación de la Comisión «i2010: Una sociedad de la Información Europea para el crecimiento y el empleo». También destaca la Directiva 2006/123/CE, relativa a los servicios en el mercado interior. Hay que resaltar la constitución del Consejo Asesor para la Administración electrónica, grupo de trabajo con expertos de prestigio en ámbitos tecnológicos que deben proponer medidas para el impulso de la Administración electrónica en España. Este grupo de trabajo tuvo el encargo de elaborar el borrador de la Ley de Administración Electrónica. Hay que destacar también la Ley Foral 11/2007, de 4 de abril, para la Implantación de la Administración Electrónica en la Administración de la Comunidad Foral de Navarra.

(19) Este plazo es una consecuencia del «Plan de acción sobre Administración electrónica i2010: Acelerar la Administración electrónica en Europa en beneficio de todos». En todo caso, hay que señalar que en el ámbito de las Comunidades Autónomas y de las Administraciones Locales la Disposición Final Tercera supedita el plazo de 31 de diciembre de 2009 a «que lo permitan sus disponibilidades presupuestarias».

La Ley 2/2011, de 4 de marzo, de Economía Sostenible, a través de su Disposición final séptima, ha añadido un nuevo apdo. 5 a la Disposición final tercera de la LAECSP donde se señala que «las Comunidades Autónomas y las Entidades integradas en la Administración Local en las que no puedan ser ejercidos a partir del 31 de diciembre de 2009 los derechos reconocidos en el artículo 6 de la presente Ley, en relación con la totalidad de los procedimientos y actuaciones de su competencia, deberán aprobar y hacer públicos los programas y calendarios de trabajo precisos para ello, atendiendo a las respectivas previsiones presupuestarias, con mención particularizada de las fases en las que los diversos derechos se-

Protección de Datos(20). Además, desde la entrada en vigor de esta Ley, las Administraciones Públicas deben hacer pública y mantener actualizada la relación de procedimientos administrativos que pueden ser gestionados de forma electrónica –Disposición final tercera de la LAECSP–.

La Administración se encuentra, de esta forma, obligada a aceptar las solicitudes electrónicas presentadas por los ciudadanos, lo que significa la generalización de la validez administrativa del documento electrónico, con la consiguiente eliminación de más de 20 millones de documentos en papel al año. La LAECSP lleva a cabo una intensa regulación de los registros electrónicos –arts. 24-26– que deroga la regulación existente de los registros telemáticos del art. 38.9 de la LRJPAC, subsistiendo la regula-

---

rán exigibles por los ciudadanos. Los anteriores programas podrán referirse a una pluralidad de municipios cuando se deban ejecutar en aplicación de los supuestos de colaboración previstos en el apartado anterior. Dos. Los programas mencionados en el apartado anterior deberán ser objeto de aprobación y publicación en el plazo de seis meses desde la entrada en vigor de la presente Ley.»

(20) Las Agencias de Protección de Datos se encuentran también obligadas en virtud de la Ley 11/2007, de 22 de junio, a facilitar a los ciudadanos la posibilidad de relacionarse con ellas por medios electrónicos por lo que deben implantar los servicios de Administración electrónica a sus procedimientos. Si bien tanto la LRJ-PAC –art. 2.2– como la LAECSP –art. 2.1.a)– hacen referencia a las Entidades de Derecho Público vinculadas o dependientes de cualquiera de las Administraciones Públicas y no a las llamadas Administraciones Independientes, hay que entender que éstas son Administraciones Públicas vinculadas que en virtud del art. 35.2 LOPD actúan en el ejercicio de sus funciones públicas de conformidad con la LRJ-PAC. La LAECSP es una regulación relativa al régimen jurídico de las Administraciones Públicas y al procedimiento administrativo común por lo que es de plena aplicación a las Agencias de Protección de Datos, lo que obliga a cumplir los plazos establecidos en la Disposición final 3ª. Así, la APDCM permite desde el año 2007 la presentación de denuncias por incumplimiento de la legislación de protección de datos y la tutela de los derechos de los ciudadanos por medios electrónicos. De hecho, esta Agencia ha facilitado que los derechos de acceso, rectificación, cancelación y oposición ante el responsable del fichero puedan ser ejercidos por los ciudadanos utilizando medios electrónicos, asumiendo la responsabilidad de este fichero. Cfr. «Presentación» a la *Memoria de la Agencia de Protección de Datos de la Comunidad de Madrid 2007*, pp. 343-346. También la Agencia de la Comunidad de Madrid puso en marcha en el año 2005 para los responsables de ficheros de titularidad pública un servicio electrónico de ayuda para el cumplimiento de sus obligaciones en materia de protección de datos personales –CUMPLE–, que permite la notificación de inscripciones de ficheros mediante certificados digitales, la elaboración de los informes de auditoría de seguridad y así como su remisión a la Agencia. Cfr. A. Troncoso Reigada, «Una actividad prestacional del derecho fundamental a la protección de datos personales: el ejemplo de la Agencia de Protección de Datos de la Comunidad de Madrid», en *Estudios sobre Comunidades Autónomas y Protección de Datos Personales*, Civitas-APDCM, 2006, pp. 286-287. La Agencia Española inició un servicio semejante de notificaciones telemáticas de los ficheros y tratamientos –Sistema NOTA– para su inscripción en el Registro General de Protección de Datos en el año 2006. Lógicamente, la entrada en vigor de la LAECSP obliga a las Agencias de Protección de Datos a determinar las condiciones e instrumentos de creación de las sedes electrónicas y las características generales del servicio, lo que puede hacerse a través de una Instrucción o de una Resolución –en el pasado la AEPD aprobó la *Instrucción* 1/2006, de 8 de noviembre, que creaba el registro telemático y aprobaba formularios–.

ción de los registros generales en soporte informático establecida en el art. 38.3 LRJAP y PAC. Esta Ley también lleva a cabo una precisa regulación de las notificaciones por medios electrónicos –art. 28–, que deroga la regulación de las antes denominadas notificaciones telemáticas establecida en el art. 59.3 de la LRJAP y PAC por la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, manteniendo la necesidad de que el interesado «haya señalado dicho medio como preferente o haya consentido su utilización». Estas notificaciones se harán mediante Internet, bien a través de una cuenta de correo electrónico del interesado –en un servidor donde el mensaje sea almacenado–, bien a través del sitio web institucional de la Administración(21).

Además del derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos, la LAESP reconoce otros derechos como el de «no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información» –art. 6.2.b) LAECSP–. Hay que recordar que el art. 35 f) de la LRJAP establecía el derecho de los ciudadanos «a no presentar documentos no exigidos por las normas aplicables al procedimiento de que se trate, o que ya se encuentren en poder de la Administración actuante». Por tanto, la LAECSP no se limita a reconocer este derecho en relación con un documento en poder de la Administración que tramita el procedimiento sino de cualquier Administración Pública. Este derecho implica facilitar los accesos electrónicos a documentos administrativos en el marco de la misma Administración Pública y las cesiones entre las distintas Administraciones Públicas(22), lo que obliga

(21) El sistema de notificación tiene que permitir acreditar la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso a su contenido, momento a partir del cual la notificación se entenderá practicada a todos los efectos legales. Si existe constancia de la puesta a disposición y transcurren diez días sin que se acceda a su contenido, la notificación se entenderá rechazada con los efectos establecidos en el art. 59.4 LRJ-PAC, salvo que de oficio o a instancia del destinatario se llegue a comprobar la imposibilidad técnica o material del acceso. Durante la tramitación del procedimiento, el interesado podrá requerir al órgano correspondiente que las sucesivas notificaciones no se practiquen por medios electrónicos. Producirá los efectos propios de la notificación por comparecencia el acceso electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia de dicho acceso. Cfr. más ampliamente A. SÁNCHEZ NAVARRO, «La articulación del derecho a la protección de datos de carácter personal en la gestión electrónica de los procedimientos administrativos», *loc. cit.,* pp. 147-149.

(22) La Exposición de Motivos señala que para hacer efectivo este derecho, se establece «la obligación de cada Administración de facilitar a las otras Administraciones los datos de los interesados que se le requieren y obren en su poder» –Apdo. VI–. La propia LAECSP reitera que «[p]ara un eficaz ejercicio del derecho reconocido en el apartado 6.2.b), cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico […]» –art. 9.1–. De hecho, la propia LAECSP establece que las Administraciones Públicas utilizarán preferentemente medios electrónicos en sus comunicaciones con otras Administraciones Públicas –art. 27.7–.

a la utilización de las tecnologías de la información en las relaciones entre las Administraciones Públicas con un nivel adecuado de interoperabilidad de los sistemas de información(23). También se reconoce el derecho a «elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas» –art. 6.2.a) LAECSP–(24). La LAECSP reconoce también el ejercicio por medios electrónicos de otros derechos que ya se encontraban en el art. 35 de la LRJAP y PAC. Así, se reconoce el derecho a «conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquéllos» –art. 6.2.b), desarrollado después en el art. 37– y a «obtener copias electrónicas de los documentos electrónicos que

(23) La LAECSP establece un «principio de cooperación en la utilización de medios electrónicos por las Administraciones Públicas al objeto de garantizar tanto la interoperabilidad de los sistemas y soluciones adoptados por cada uno de ellas como, en su caso, la prestación conjunta de servicios a los ciudadanos» –art. 4.e)–. El Anexo de la LAECSP –apdo. o)– define interoperabilidad como «capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de operación y conocimiento entre ellos». La LAECSP establece un Comité Sectorial de Administración electrónica que tiene como una de sus funciones «asegurar la compatibilidad e interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones Públicas» –art. 40.2.a)–. Así, se prevé la creación de un Esquema Nacional de Interoperabilidad que comprenda un conjunto de criterios y recomendaciones para la toma de decisiones tecnológicas que garanticen esta interoperabilidad –aprobado por el Real Decreto 4/2010, de 8 de enero–. Se trata de crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas Españolas. Cfr. el Capítulo II de la LAECSP –arts. 41-43– sobre la cooperación en materia de interoperabilidad de sistemas y aplicaciones. Cerrillo ha señalado que dado el carácter poliédrico de la Administración electrónica no es suficiente el establecimiento de criterios técnicos compartidos entre las diferentes Administraciones que permitan la interconexión sino que hace falta un liderazgo político suficiente que impulse los cambios organizativos necesarios para poder abordar dicha interrelación. Es necesario que existan unas normas y reglas que permitan adaptar criterios comunes –la gobernanza de la interoperabilidad– y un marco institucional que posibilite la cooperación entre Administraciones Públicas, el intercambio de estándares y la definición de protocolos que hagan posible esta interoperabilidad. Cfr. A. Cerrillo i Martínez, «La interoperabilidad y la protección de datos. La interconexión de los registros de protección de datos», en AA VV, *La protección de datos en la Administración electrónica*, Aranzadi, Cizur Menor, 2009, pp. 23-57. La interoperabilidad de los distintos Registros de ficheros de las Agencias de Protección de Datos –Española y Autonómicas– es una cuestión que hemos analizado en otro momento. Cfr. A. Troncoso Reigada, «Las Comunidades Autónomas y la protección de datos personales a la luz de las reformas estatutarias», en *Estudios sobre Comunidades Autónomas y Protección de Datos Personales*, Civitas-APDCM, Madrid, pp. 122-138.

(24) La LAECSP contiene un Anexo de definiciones entre las que se encuentra la de canales –apdo. c)–: «Estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, TDT, etc.)». Como señala la Exposición de Motivos, el ordenador e Internet pueden ser una vía pero no es la única; hay que destacar también las comunicaciones via SMS y la propia Televisión Digital Terreste –apdo. III–.

formen parte de procedimientos en los que tengan la condición de interesado» –art. 6.2.e)–, que se encontraban previstos en el art. 35.a) y c) LRJAP y PAC. También se reconocen otros derechos como el de «la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente» –art. 6.2.f)–, el de «obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública» –art. 6.2.g)–, el de «la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas» –art. 6.2.h)–, el de «la calidad de los servicios públicos prestados por medios electrónicos» –art. 6.2.j)– y el de «elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos» –art. 6.2.k)–.

La regulación del derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos tiene un carácter básico ya que va destinada a permitir un tratamiento común de los ciudadanos con las Administraciones Públicas(25). Es competencia exclusiva del Estado las bases del régimen jurídico de las Administraciones Públicas que garantiza a los administrados un tratamiento común ante ellas y el procedimiento administrativo común, todo ello sin perjuicio de las especialidades derivadas de la organización propia de las Comunidades Autónomas –art. 149.1.18 CE–, lo que significa que la regulación del acceso electrónico a los servicios públicos debe respetar la distribución competencial entre el Estado y las CC AA y, especialmente, las competencias de autoorganización. Esta Ley reconoce y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas «con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica» –art. 1 LAECSP–. Como señala la Exposición de Motivos, «la regulación del Estado debe abordar aquellos aspectos en los que es obligado que las previsiones normativas sean comunes, como es el caso de la interoperabilidad, las garantías de las comunicaciones electrónicas, los servicios a los que tienen derecho los ciudadanos, la conservación de las comunicaciones electrónicas y los demás temas que se abordan en la ley para garantizar que el ejercicio del derecho a relacionarse electrónicamente con to-

(25) La Disposición final primera establece los preceptos de la Ley que tienen un carácter básico. Sobre el alcance del título competencial del Estado, cfr. E. GAMERO, «Objeto, ámbito de aplicación y principios generales de la Ley de Administración Electrónica; su posición en el Sistema de Fuentes», en E. GAMERO CASADO y J. VALERO TORRIJOS (Coord.), *La Ley de Administración Electrónica*, cit., pp. 69-79.

das las Administraciones forme parte de ese tratamiento común que tienen» –apdo. II–. Sin embargo, se echa en falta una mayor coordinación entre la LAECSP y la LRJAP y PAC ya que es la integración con esta segunda Ley lo que realmente garantiza la existencia de un auténtico procedimiento administrativo común.

La LAECSP no olvida que la tramitación telemática tiene que venir precedida de un esfuerzo por alcanzar una mayor simplificación administrativa. Así, una de las finalidades de la Ley es «simplificar los procedimientos administrativos» –art. 3.6 LAECSP–. Además, uno de los principios de la Ley es de «simplificación administrativa, por el cual se reduzcan de manera sustancial los tiempos y plazos de los procedimientos administrativos, logrando una mayor eficacia y eficiencia en la actividad administrativa» –art. 4.j)–(26). Por ello se establece que la utilización de medios electrónicos en la gestión de los procedimientos, procesos y servicios no es algo aislado sino que es el último paso después de la realización de un análisis de rediseño funcional y simplificación del procedimiento, proceso o servicio en el que se considerará especialmente «la supresión o reducción de la documentación requerida a los ciudadanos, mediante su sustitución por datos, transferencias o certificaciones, o la regulación de su aportación al finalizar la tramitación, [...], la reducción de los plazos y tiempos de respuesta, [y] la racionalización de la distribución de las cargas de trabajo y de las comunicaciones internas» –art. 34–(27).

Lógicamente, las nuevas tecnologías plantean también riesgos y amenazas. Uno de los principales es que éstas supongan el establecimiento de una nueva barrera que separe el primer mundo y el tercer mundo. No olvidemos que la mitad de la población mundial no ha hecho nunca una llamada telefónica o que Nueva York tiene más terminales eléctricos que toda Africa. No obstante, las tecnologías de la información también pueden ser un elemento que contribuya a reducir el espacio que separa a los países menos desarrollados de los más desarrollados. Estonia puede ser un buen ejemplo de lo que estamos diciendo.

El recurso a las nuevas tecnologías no debe perjudicar la relación

(26) La simplificación administrativa también se cita como criterio para impulsar la aplicación de medios electrónicos a los procesos de trabajo y la gestión de los procedimientos y de la actuación administrativa –art. 33.1– y como uno de los elementos que debe garantizar las aplicaciones y sistemas de información utilizados para la instrucción por medios electrónicos –art. 36.1–. En todo caso, la LAECSP no modifica la regulación de las disposiciones generales sobre el procedimiento administrativo contempladas en el Título IV de la LRJ-PAC. Como señala Sánchez Navarro, el recurso de la Administración a las nuevas tecnologías así como la mayor simplificación administrativa también deberían suponer una reducción de los plazos para algunos procedimientos establecidos en la LRJ-PAC. Cfr. A. SÁNCHEZ NAVARRO, *loc. cit.*, p. 107.

(27) La necesidad de rediseñar y simplificar los procedimientos administrativos con anterioridad a su automatización era una cuestión sobre la que habíamos incidido tempranamente en «Las Cartas de Servicio: un compromiso con el ciudadano», cit.

con los ciudadanos. Por ello, la Administración, además de apostar por la participación a través de los nuevos canales de comunicación, tiene que mejorar la atención presencial, a través del establecimiento o la remodelación de las oficinas de información y atención a los ciudadanos –eliminación de barreras, acondicionamiento de oficinas, establecimiento de gestores de turnos, etc.–, y fortalecer la atención telefónica(28). Hay que señalar que el art. 6.2.c) de la LAECSP reconoce el derecho «a la igualdad en el acceso electrónico a los servicios de las Administraciones Públicas», lo que significa que ni el recurso a los medios electrónicos para relacionarse con las Administraciones Públicas ni la negativa a utilizarlos puede suponer el establecimiento de una discriminación o de una limitación de acceso a los servicios públicos(29). De hecho, la utilización de medios electrónicos para comunicarse con la Administración es, como regla general, una opción del ciudadano –que debe haberlo solicitado o consentido expresamente– y no una obligación que pueda imponer la Administración. Únicamente la LAECSP prevé la obligatoriedad de comunicación con las Administraciones Públicas a través de medios electrónicos «cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos» –art. 27–(30). No obstante, la necesidad de garantizar la igualdad de los ciudadanos cualquiera que sea la forma de tramitación –en papel o electrónica– podría implicar que uno de los criterios para imponer la tramitación electrónica es que no sea posible garantizar esta igualdad. Además, la Administración está obligada a facilitar a todos el acceso a las nuevas tecnologías, no sólo mediante una actividad formativa –orientada principalmente a los ciudadanos de mayor edad, sino también mediante el establecimiento de puntos de acceso electrónico en el ámbito de las Administraciones Públicas(31), así como a través de medi-

(28) Como señala la Exposición de Motivos de la LAECSP, «el uso de los medios electrónicos no puede significar merma alguna del derecho del interesado en un expediente a acceder al mismo en la forma tradicional». La apuesta por las nuevas tecnologías no tiene que hacernos olvidar la atención presencial, porque las personas mayores siempre irán a una oficina de atención a los ciudadanos y allí deberán encontrar un lugar luminoso, accesible, con ausencia de obstáculos, con gestores de turnos, etc. Cfr *Manual de Acogida y Atención al Ciudadano de la Comunidad de Madrid*, Dirección General de Calidad de los Servicios, Comunidad de Madrid-Coopers and Lybrand, 1997.

(29) La LAECSP establece como principio general el «principio de igualdad con objeto de que en ningún caso el uso de medios electrónicos pueda implicar la existencia de restricciones o discriminaciones para los ciudadanos que se relacionen con las Administraciones Públicas por medios no electrónicos» –art. 4.b)–.

(30) Esta obligatoriedad que puede comprender también la práctica de notificaciones administrativas por medios electrónicos así como la necesaria utilización de los registros electrónicos que se especifiquen, pueden establecerse mediante orden ministerial publicada en el BOE y en la sede electrónica –art. 32 Real Decreto 1671/2009, de 6 de noviembre–.

(31) En esta dirección, el art. 8 de la LAECSP «Garantía de prestación de servicios y disposición de medios e instrumentos electrónicos» obliga a las Administraciones

das técnicas que favorezcan la accesibilidad para las personas que tengan algún tipo de discapacidad(32). Además, las nuevas tecnologías no deben ser el único cauce para la participación social, para no perjudicar a los grupos sociales que no las utilizan(33). La LAECSP afirma también una suerte de principio de igualdad para los usuarios y proveedores de tecnologías de la información y comunicación, «el principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicas» que busca garantizar «la independencia en la elección de las alternativas tecnológicas por los ciudadanos y por las Administraciones Públicas, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos las Administraciones Públicas utilizarán estándares abiertos así como en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos» –art. 4.i)–. Por tanto, el legislador no se inclina por alguna tecnología concreta existente sino que permite todas aquellas que existan o puedan existir en el futuro(34). Este principio de neutralidad tecnológica persigue, como señala la Exposición de Motivos del Real Decreto 1671/2009, de 6 de noviembre, evitar que la implantación de la LAECSP «imponga una renovación tal en las soluciones de comunicación con los ciudadanos que impida la pervivencia de técnicas existentes y de gran arraigo»; «facilitar la actividad de implantación y adaptación de la

---

a habilitar canales y medios para la prestación de los servicios electrónicos, garantizando el acceso a todos los ciudadanos con independencia de sus circunstancias personales, medios o conocimientos. La Administración General del Estado ofrece a este respecto varios canales como las oficinas de atención presencial –que ofrecen asistencia y orientación sobre su utilización–, los puntos de acceso electrónicos gestionados por los departamentos y el servicio de atención telefónica. Esto obliga a una especial formación en protección de datos de los empleados públicos que atienden al público, una cuestión a la que hace mención el apdo. III de la Exposición de Motivos y la Disposición Adicional Segunda. En otro orden de cosas, la Exposición de Motivos de la LAECSP afirma que el derecho de los ciudadanos a relacionarse con la Administración a través de medios electrónicos supone dentro de Internet «la obligación de poner a disposición de ciudadanos y empresas al menos un punto de acceso general a través del cual los usuarios puedan, de forma sencilla, acceder a la información y servicios de su competencia; presentar solicitudes y recursos; realizar el trámite de audiencia cuando proceda; efectuar pagos o acceder a las notificaciones y comunicaciones que les remitan la Administración Pública» –apdo. II–.

(32) La LAECSP proclama así un principio de accesibilidad a la información –art. 4.c)–.

(33) En todo caso, como hemos indicado anteriormente, el modelo tradicional de participación social dista de ser transparente y se presta a la actividad de grupos de presión.

(34) Este principio también se encuentra en el art. 3.f) de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones que proclama la necesidad de «fomentar, en la medida de lo posible, la neutralidad tecnológica en la regulación» y en la Directiva 2002/58/CE, de 12 de julio de 2002, del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que obliga a los Estados miembros a velar «porque no se impongan requisitos obligatorios respecto de características técnicas específicas a los equipos terminales u otros equipos de comunicaciones electrónicas que puedan obstaculizar la puesta en el mercado de dichos equipos y su libre circulación en los Estados miembros» –art. 14.1–.

LAECSP a las distintas organizaciones, funciones y procedimientos a los que es de aplicación»; e «impedir que la opción rígida por determinadas soluciones dificulte para el futuro la incorporación de nuevas soluciones y servicios». Lógicamente, el respeto al pluralismo y la existencia de un marco flexible en las opciones tecnológicas queda delimitado por la obligación de respetar las medidas de seguridad que se establecen en la Ley y en la legislación de protección de datos personales.

II. LA PROTECCIÓN DE DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA

El riesgo más importante de la Administración electrónica es que suponga una vulneración del derecho fundamental a la protección de datos personales(35). Las personas son cada vez más conscientes y cautelosas con sus datos personales y tienen una mayor sensibilidad acerca de su protección, una sensibilidad que se ve incrementada con la implantación de la Administración electrónica. No olvidemos que nuestra Constitución obliga especialmente a los poderes públicos a limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos –art. 18.4 CE–. Como hemos señalado en otro momento, el derecho fundamental a la protección de datos personales no trata de impedir el recurso a las nuevas tecnologías sino de conciliarlo con el respeto a la dignidad de la persona. Si bien la actividad de la Administración Pública debe orientarse al principio de eficacia, dicho principio no debe ser interpretado de forma independiente sino en consonancia con todo el ordenamiento jurídico y con los derechos fundamentales.

1. EL INCREMENTO DE LOS TRATAMIENTOS DE DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA

La utilización de medios y técnicas electrónicas, informáticas y telemáticas por las Administraciones Públicas lleva aparejado el almacena-

(35) Cfr. recientemente AA VV, *La protección de datos en la Administración Electrónica*, Aranzadi, Cizur Menor, 2009, especialmente J. VALERO TORRIJOS, «Implicaciones de la protección de datos de carácter personal para la Administración electrónica», pp. 177-198. Como referencias generales, cfr. M. FERNÁNDEZ SALMERÓN, *La protección de los datos personales en las Administraciones Públicas*, Civitas, Madrid, 2003; E. GUICHOT, *Datos personales y Administración Pública*, Civitas, Madrid, 2005; J. VALERO TORRIJOS y M. FERNÁNDEZ SALMERÓN, «Protección de datos personales y administración electrónica», *Revista Española de Protección de Datos*, nº 1, 2006, pp. 115-142; J. VALERO TORRIJOS y J. A., PELLICER, «Algunas consideraciones sobre el derecho a la protección de los datos personales en la actividad administrativa», *Revista Vasca de Administración Pública*, nº 59, 2000, pp. 255-288; J. VALERO TORRIJOS, «El uso de cookies por las Administraciones Públicas: ¿una vulneración de la normativa sobre protección de los datos personales?», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 3, 2003, pp. 173-178. Hay que destacar también el trabajo de A. SÁNCHEZ NAVARRO, «La articulación del derecho a la protección de datos de carácter personal en la gestión electrónica de los procedimientos administrativos», *Revista Española de Protección de Datos*, nº 3, 2007, pp. 95-169. Cfr. también con

miento y tratamiento automatizado de la información personal pues en caso contrario perdería sentido el recurso a este tipo de medios y técnicas. Esto es especialmente evidente cuando se pone en marcha la tramitación electrónica de los procedimientos administrativos(36). Así, la posibilidad de iniciar procedimientos administrativos a través de Internet, aunque después se proceda al almacenamiento manual de la información, obliga a la existencia de los correspondientes registros electrónicos –para la recepción o salida de las solicitudes, escritos y comunicaciones–(37). La Administración Pública puede optar por una tramitación completa por medios electrónicos –el expediente electrónico al que hace referencia el art. 32 de la LAECSP debe ser considerado también un fichero de datos de carácter personal– o por una tramitación parcial por medios electrónicos, imprimiendo documentos en soporte papel, lo que supone un tratamiento mixto o parcialmente automatizado. También es un tratamiento automatizado de datos personales la creación, gestión y mantenimiento de repositorios de información o documentales, para su uso por diferentes órganos de la misma o de distinta Administración Pública, un servicio horizontal que permite a los ciudadanos el ejercicio de los derechos previstos en la LAECSP.

Además, la utilización de las nuevas tecnologías para prestar otros servicios complementarios también supone un incremento de los tratamientos de datos personales realizados por las Administraciones Públicas. Esto ocurre, por ejemplo, con la puesta en marcha de herramientas como la recepción de información o de sugerencias y reclamaciones de los ciudadanos a través de una dirección institucional de correo electrónico, donde se lleva a cabo frecuentemente un tratamiento de datos relativos al nombre, apellidos y dirección de correo electrónico, etc.–. Igualmente, la recogida de *cookies* –o cualquier otro mecanismo de seguimiento– representa un tratamiento de datos personales(38), sin perjuicio del derecho a la información y el consentimiento del interesado al que después nos referiremos. Si bien la dirección IP no siempre es estática sino que puede ser dinámica, además de que no identifica a un usuario sino un

---

el *Libro Blanco sobre la Administración electrónica y la protección de datos personales*, Documentos INAP, nº 27, 2003, 109 pp.

(36) Salvador Carrasco destaca que la aplicación de la LAECSP implica la automatización de los siguientes procesos: información, iniciación electrónica, pago electrónico, notificaciones y comunicaciones electrónicas y consulta del estado de tramitación. Cfr. L. De Salvador Carrasco, «Retos de la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos para la Agencia Española de Protección de Datos», en AA VV, *La protección de datos en la Administración Electrónica*, cit., pp. 199-217.

(37) Los registros electrónicos pueden admitir no sólo documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen en la norma de creación del registro y bajo un formato preestablecido sino también cualquier solicitud, escrito o comunicación dirigido a cualquier órgano o entidad del ámbito de la Administración titular del registro –art. 24.2 LAECSP–.

(38) Las *cookies*, con independencia de la información almacenada en las mismas, pueden vincularse con el usuario de un determinado dispositivo conectado a Internet y permite obtener el perfil del mismo.

equipo –que puede ser de utilización compartida–(39), en muchas ocasiones es una «información concerniente a personas físicas identificadas o identificables» –art. 3.a) LOPD–(40). También suponen tratamientos de datos personales otros servicios de Administración electrónica fuera

(39) Pensemos en un ordenador de un punto de acceso público a Internet o de un cibercafé, que no puede asociarse de manera unívoca a una persona.

(40) Cfr. E. ACED, «¿Es la dirección IP un dato de carácter personal?», en *Datospersonales.org Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº 13, 2005. El Grupo de Trabajo del Artículo 29 ha señalado que la dirección IP (estática o dinámica) asignada a un dispositivo conectado a Internet tiene la consideración de dato de carácter personal, al poder ser identificado el usuario, por medios razonables, tanto por los proveedores de acceso a Internet como por los administradores de redes de área local. Cfr. el documento de trabajo sobre «Privacidad en Internet: Enfoque comentario integrado de la protección de datos en línea», adoptado el 21 de noviembre de 2000, pp. 9-11 –*http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37es.pdf*–. Como señala la Agencia Española de Protección de Datos en el Informe 327/2003 –accesible en su web–, «[e]l TCP/IP es un protocolo básico de transmisión de datos en Internet, donde cada ordenador se identifica con una dirección IP numérica única. Las redes TCP/IP se basan en la transmisión de paquetes pequeños de información, cada una de los cuales contiene una dirección IP del emisor y del destinatario. Por otro lado, el DNS (sistema de nombre de dominio) es un mecanismo de asignación de nombres a ordenadores identi ficados con una dirección IP. Ciertas herramientas existentes en la red permiten encontrar el enlace entre el nombre de dominio y la empresa o el particular. A su vez, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP. Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet, normalmente mantiene un fichero histórico con la dirección IP (fija o dinámica) asignada, el número de identificación del suscriptor, la fecha la hora y la duración de la asignación de dirección. Es más, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación. En estos casos, ello significa que, con la asistencia de terceras partes responsables de la asignación, se puede identificar a un usuario de Internet, es decir, obtener su identidad civil (nombre dirección, número de teléfono, etc.), por medios razonables, con lo que no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 3 de la Ley 15/1999. En otros casos, un tercero puede llegar a averiguar la dirección IP dinámica de un usuario pero no ser capaz de relacionarla con otros datos que le permitan identificarlo. Obviamente, resulta más sencillo identificar a los usuarios de Internet que utilizan direcciones estáticas. Sin embargo, en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como cookies con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permite su identificación. *Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos*» [la cursiva es nuestra]. Esta doctrina es transcrita en la Resolución R/400/2006, de AEPD, donde se analiza la solicitud de acceso a información relativa a la dirección o direcciones IP asignadas a las conexiones a Internet, así como a los datos de tráfico durante un período determinado, alegando el

del ámbito de los procedimientos administrativos como los servicios de novedades o de noticias –*newsletter*– o los servicios de alertas a través de mensajes SMS que son ficheros de datos personales –al menos del correo electrónico o del teléfono móvil–. La web 2.0 ha posibilitado también que se recojan datos personales en procesos de participación social por medios electrónicos –donde se solicita a los ciudadanos su opinión sobre distintas actuaciones administrativas– o en foros de discusión para usuarios y para empleados públicos en sitios web institucionales(41).

Es importante resaltar que la utilización de medios electrónicos transforma en un tratamiento de datos personales –en este caso automatizado– algo que no siempre era un fichero o un tratamiento manual-estructurado –ya que a veces se trata de una información administrativa en papel que no se encuentra estructurada de conformidad con personas–. Esto es lo que ocurre con la facturación electrónica –en muchas ocasiones las facturas en papel no se encuentran ordenadas de conformidad con personas–(42). Lo mismo puede decirse de la publicación en Internet de información administrativa donde se contengan datos de «personas físicas identificadas o identificables» –art. 3.a) LOPD– y que suponen una cesión de datos personales(43), algo que no puede aplicarse igualmente

---

art. 12 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico que obliga a los operadores de redes y proveedores de acceso a retener los datos de conexión por un período máximo de doce meses. La empresa manifestó que los datos solicitados se encuentran cancelados, conforme a lo establecido en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), que obliga a cancelar aquellos datos que no se ajusten a la finalidad para la que fueron obtenidos. Por tanto, se tramita como una solicitud de acceso a datos personales aquella referida a la dirección IP. Como señala la Agencia Española, «[d]e este modo, las cuestiones planteadas en el presente procedimiento deberán resolverse atendiendo a lo dispuesto, con carácter general, en la LOPD, a la que está sometido el ejercicio de la actividad desarrollada por los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de esta naturaleza, por virtud del artículo 34 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (en lo sucesivo LGT), según el cual «... *los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal conforme a la legislación vigente*».

(41) Lógicamente, no hay tratamiento de datos personales si esta participación es anónima o a través de un seudónimo que no haga identificable a la persona y no se recoge la dirección IP.

(42) Este planteamiento en lo relativo a la facturación electrónica se ha visto afectado por las excepciones al ámbito objetivo de aplicación del Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, en lo que hace referencia a los datos de las personas físicas que prestan servicios en personas jurídicas –cuando consistan en su nombre, apellidos, funciones o puestos desempeñados así como la dirección postal o electrónica, teléfono y número de fax profesional– y a los datos relativos a empresarios individuales cuando se haga referencia a ellos en su calidad de comerciantes, industriales o navieros –art. 2.3 y 4–. Ésta es una cuestión que hemos analizado en nuestra «Introducción y Presentación» a *Protección de datos personales para Administraciones Locales*, Civitas-APDCM, Madrid, 2008, pp. 22-27.

(43) Como es sabido, la LOPD se aplica a los datos de carácter personal registrados en soporte físico y que sean susceptibles de tratamiento –art. 2–. La publicación en Internet supone un tratamiento automatizado

a la publicación de información administrativa en papel que no se encuentre estructurada de conformidad con personas(44). Esto ocurre, por ejemplo, con los Boletines y Diarios Oficiales en papel que no son un fichero manual –la información no se encuentra estructurada de conformidad con personas de forma que la localización del dato personal se produzca sin esfuerzos desproporcionados– pero la versión electrónica sí es un tratamiento –en este caso, automatizado– de datos personales –basta poner un dato personal en un buscador general o en el de la propia edición electrónica del boletín para que se produzca la accesibilidad inmediata a la información–(45). Así, la publicación en la página web de un Ayuntamiento de las sesiones y acuerdos del Pleno de Corporaciones Locales –una previsión que se encuentra en el art. 70 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local y que debe ser desarrollada en el Reglamento Orgánico de cada Ayuntamiento– supone un tratamiento –una cesión– de datos de carácter personal(46). Además, si bien el derecho fundamental a la protección de datos protege también los tratamientos en papel –los ficheros manual-estructurados–, no es lo mismo la utilización de medios electrónicos en lugar de los medios tradicionales para el almacenamiento de la información personal.

2. LA PROTECCIÓN DE DATOS PERSONALES COMO OPORTUNIDAD PARA LA ADMINISTRACIÓN ELECTRÓNICA

Los principios y derechos de protección de datos son plenamente aplicables a los tratamientos de datos personales en los servicios de Administración electrónica(47). Este derecho fundamental tiene como objeto

---

en virtud de la definición de tratamiento de datos contenida en el art. 3.c) de la LOPD ya que se trata de una operación y procedimiento técnico de carácter automatizado que permite las cesiones de datos.

(44) El concepto de tratamiento de datos personales y la distinción entre el tratamiento automatizado y el manual ha sido analizado en «La comunicación de datos personales», en A. TRONCOSO REIGADA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas-Thomson-Reuters, Cizur Menor, 2010, pp. 950-959.

(45) El hecho de que los boletines y diarios oficiales tengan el carácter de fuente accesible al público en virtud del art. 3.j) de la LOPD y del art. 7 del Reglamento de desarrollo supone una excepción especifica al consentimiento del interesado para el tratamiento y para la cesión –arts. 6.2 y 11.2.c) LOPD– pero no los excluye del ámbito de aplicación de la LOPD.

(46) La publicación de información personal en diarios oficiales y en sitios web ha sido analizado en «Transparencia administrativa y protección de datos personales», cit., pp. 23-188. Cfr. también la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre Publicación de Datos Personales en Boletines y Diarios Oficiales en Internet, en sitios Webs Institucionales y en otros Medios Electrónicos y Telemáticos.

(47) Quisiera destacar especialmente el libro *e-PRODAT: Administración electrónica y Protección de Datos en Regiones y Ciudades Europeas* –Madrid, 2006–, que recoge las conclusiones más sobresalientes de un Proyecto Europeo dirigido por la Agencia de Protección de Datos de la Comunidad de Madrid y en el que han participado diferentes Administraciones Públicas de la Unión Europea. Este proyecto europeo e-Prodat -enmarcado dentro del plan de acción e-Europe 2005, que tenía como objetivos la ciberseguridad y el establecimiento de servicios públicos interactivos para todos–, trató de promover el derecho fundamental a la

la información sometida a tratamiento de personas físicas, no de personas jurídicas, por lo que no existe obstáculo en este ámbito para el tratamiento de datos de personas jurídicas por los servicios de Administración electrónica. En todo caso, se puede afirmar que no sólo es posible hacer compatibles la eficacia e inmediatez de los servicios de Administración electrónica y el respeto al derecho fundamental a la protección de datos de carácter personal. Aún más: sólo si protegemos los datos personales podemos establecer la relación de confianza necesaria para el desarrollo de las nuevas tecnologías de la información y la comunicación en la socie-

---

protección de datos personales en los servicios de Administración electrónica. Para alcanzar sus objetivos, e-Prodat puso el acento en la importancia del intercambio de conocimientos y experiencias en este ámbito. Este libro identificó un conjunto de mejores prácticas, llevando a cabo una evaluación sobre protección de datos y Administración electrónica en las regiones y ciudades europeas, que se desglosaría tanto en una evaluación del grado de penetración de las nuevas tecnologías en las Administraciones Públicas Europeas –cuál es el estado de los servicios públicos de administración electrónica en regiones y ciudades europeas– como en el estudio del nivel de respeto al derecho fundamental a la protección de datos personales por parte de estos servicios de Administración electrónica. Esta evaluación se realizó sobre la base de un conjunto de indicadores relativos a la calidad de los servicios de Administración electrónica, la adecuación de la infraestructura de telecomunicaciones para la prestación de estos servicios, la existencia de un adecuado capital humano, la presencia de mecanismos para fomentar la participación ciudadana a través de las nuevas tecnologías, la voluntad de alcanzar la excelencia en la Administración electrónica y la seguridad y el cumplimiento de la normativa en protección de datos. Están especialmente bien diseñados los índices de medición de los servicios de Administración electrónica, que parten de la mera presencia administrativa en Internet de manera de manera estática y dinámica, a las posibilidades interactivas de envío de solicitudes y pago de impuestos, hasta la presencia transaccional y en red que permite la realización de múltiples tareas *on line* e intereacciones bidirecionales con los ciudadanos, permitiendo a éstos tomar parte en la toma de decisiones públicas. De la evaluación se dedujo la enorme heterogeneidad dentro de Europa en relación con las infraestructuras de telecomunicación, el gobierno electrónico, la participación electrónica y la protección de datos en la Administración electrónica. Existe, en cambio, una mayor homogeneidad en lo que respecta a la educación y a la formación. También se concluyó la existencia de un régimen jurídico similar relativo a la protección de datos con independencia de que los países pertenezcan o no a la Unión Europea. No obstante, hay una desigualdad en lo relativo a la presencia de una legislación sectorial que regule determinadas actividades de la manera más adecuada a las circunstancias concretas y que resuelva los problemas de protección de datos. Es especialmente importante una legislación específica sobre protección de datos adaptada al área de las telecomunicaciones como ocurre en la Unión Europea. Existe un nivel adecuado de homogeneidad en lo que hace referencia a la proclamación del principio de información y de consentimiento, a la protección de los datos sensibles, al establecimiento de medidas de seguridad y a las autoridades de control. El Informe finaliza con un conjunto de recomendaciones: invertir en infraestructuras de telecomunicación; promover todavía más el gobierno electrónico y los servicios de participación electrónica; facilitar el acceso de los ciudadanos a las tecnologías de la información; impulsar la protección de la privacidad de los usuarios de redes, específicamente de las páginas web de Administración y participación electrónica; difundir la cultura de la protección de datos entre las Administraciones Públicas y los ciudadanos. Entre las conclusiones más importantes se encuentra la conveniencia de desarrollar una plataforma conjunta de Administración y participación electrónica a nivel europeo.

dad y en las Administraciones Públicas(48). Por tanto, para que la Administración electrónica se implante y se desarrolle, es necesario respetar la legislación de protección de datos personales. Pues bien, además hay que señalar que la Administración electrónica, como trataremos de explicar en estas páginas, lejos de ser un obstáculo, es una ocasión para mejorar el cumplimiento de los principios y derechos de protección de datos en la Administración Pública. Las nuevas tecnologías son una oportunidad histórica para fortalecer la Administración y para mejorar el respeto al derecho fundamental a la protección de datos personales dentro de la Administración.

La Ley 24/2001, de 27 de diciembre, de medidas fiscales, administrativas y de orden social, que modifica la LRJAP y PAC, llevó a cabo ya una referencia a la legislación de protección de datos personales en el ámbito de la Administración electrónica. Así, esta Ley incorporó una Disposición adicional decimoctava –derogada por la LAECSP– relativa a la presentación telemática de solicitudes dirigidas a la Administración General del Estado y sus Organismos Autónomos, donde se señalaba –apdo. 4– que «[l]o dispuesto en la presente disposición referida se ajustará a lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en la presente Ley, en la vigente normativa sobre firma electrónica y en las correspondientes normas de desarrollo». También la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, que es aplicable a las comunicaciones con las Administraciones a través de Internet, establece que «los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal conforme a la legislación vigente» –art. 34.1–(49). En la misma dirección, la Ley 56/2007, de 28 de diciembre de Medidas de Impulso de la Sociedad de la

(48) Sobre la cuestión existe un interesante Documento de trabajo del Grupo de Protección de datos del art. 29, relativo a la Administración en línea, adoptado el 8 de mayo de 2003 –*http://www.europa.eu.int/comm/privacy*–. Ese documento fue elaborado por la delegación francesa y recoge las respuestas ofrecidas por las Autoridades de protección de datos representadas en el Grupo de trabajo a un cuestionario sobre el tema. Este documento aborda cuestiones como el establecimiento de puntos de entrada únicos a los servicios de administración en línea, la creación de identificadores únicos y la interconexión de las bases de datos públicas. Cfr. también J. VALERO TORRIJOS y F. J. SANZ LARRUGA, «E-Administración, identificación del ciudadano y protección de datos personales en la Unión Europea: ¿una ecuación posible?», que se encuentra en la web de la Agencia Catalana de Protección de Datos –*http://www.apdcat.net*–. Con anterioridad hay que destacar otro importante documento de trabajo del Artículo 29 «Privacidad e Internet: enfoque comunitario integrado de la protección de datos en línea», de 21 de noviembre de 2000.

(49) Igualmente, el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios establece en el art. 17 la obligación de «[g]arantizar la protección de los datos personales y la intimidad de las personas, conforme a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley 32/2003, de 3 de noviembre, y en su normativa de desarro-

Información, señala que «será de aplicación al tratamiento y conservación de los datos necesarios para la facturación electrónica lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo» –art. 1.5–. No obstante, en el ámbito de la Administración electrónica no parecía suficiente que la normativa contuviera una simple remisión a la legislación de protección de datos personales, cuyos principios y derechos no pueden ser afectados; era también necesaria una regulación específica que, abordando la Administración electrónica, estableciera a través de medidas concretas la vigencia y aplicación de los principios y derechos de protección de datos personales en este ámbito(50).

---

llo». Hay múltiples menciones en este Real Decreto a la legislación de protección de datos en este Reglamento.

(50) La aplicación del derecho fundamental a la protección de datos personales al ámbito de la Administración electrónica ha sido calificado por GUICHOT como «un atrevimiento casi suicida», porque se trata de «dos grupos normativos que están aún en una fase de construcción por no decir de balbuceo, que es la protección de datos –no ya aplicada a la Administración electrónica, sino en general–, y la Administración electrónica, que estamos comenzando a intuir qué puede ser. Y claro, lo que intentamos es conectar ambas, con lo cual es la dificultad de la dificultad». Cfr. E. GUICHOT REINA, «Intervención en el debate», AA VV, *La Administración electrónica*, cit., p. 248. Por ello, la APDCM aprobó la Recomendación 3/2008, de 30 de abril, de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica, que trata de establecer un conjunto de criterios para que los tratamientos de datos de carácter personal necesarios para la prestación de servicios de Administración electrónica respeten el derecho fundamental a la protección de datos. Específicamente esta Recomendación analiza la responsabilidad de los distintos tratamientos de datos personales, diferenciando claramente los supuestos de gestión y tramitación de los servicios por los órganos específicos en quienes reside la competencia, de aquellas herramientas de Administración electrónica de carácter horizontal, como son las sedes electrónicas, los portales de acceso a los servicios o los repositorios documentales, que dan servicio a diferentes órganos de una Administración para facilitar los intercambios de información previstos en la LAECSP. Además, la Recomendación establece un conjunto de criterios relativos a la política de privacidad, la suscripción de noticias, suscripción a bolsas de empleo, «chats» institucionales, procesos de participación electrónica, foros de opinión, etcétera.

Igualmente, la APDCM llevó a cabo un Plan de Inspección sobre los servicios de Administración electrónica y la política de privacidad en las Corporaciones Locales de la Comunidad de Madrid durante el año 2008 –en virtud de la habilitación prevista en el art. 18 del Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de las funciones de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal–. Este Plan analizó el grado de cumplimiento de los principios y derechos de protección de datos en la recogida y tratamiento de datos personales a través de Internet. Así, se analizaron los sitios web de los Ayuntamientos –se determinó la dirección URL del organismo inspeccionado– y se verificaron las herramientas que permitían la recogida de datos a través de formularios u otros instrumentos como buzones electrónicos y la cláusula de privacidad. A partir de la constatación de estos elementos se realizaron las siguientes comprobaciones: principio de calidad –datos que se recababan, finalidad para la que estaban siendo recabados, y proporcionalidad (valoración si eran datos excesivos)–; principio de información –verificación de si se incluía información a la que se refiere el artículo 5 de la LOPD–; datos especialmente protegidos; cesiones de datos –relación de organismos cedentes; justificación de la cesión; finalidad de la cesión–; acceso a datos por cuenta de terceros –valoración de su existencia a

Así, la Exposición de Motivos de la LAECSP reconoce la necesidad de crear un marco jurídico que, al tiempo que facilita la extensión de las tecnologías de la información y la comunicación en la Administración, sea capaz de generar la suficiente confianza para eliminar o minimizar los riesgos asociados a su utilización, especialmente los relativos a la pérdida de privacidad y a la escasa transparencia de estas tecnologías –apdo. V–. De hecho, la LAECSP señala como uno de sus fines la creación de condiciones de confianza en el uso de estas tecnologías, estableciendo las medidas necesarias para «la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y servicios electrónicos» –art. 3.3–. Esta regulación sectorial que trata de materializar los principios y derechos de protección de datos personales en los servicios de Administración electrónica, como señala la Exposición de Motivos de la LAECSP, no pretende hacer ninguna innovación en relación con la normativa de protección de datos contenida en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sino que ésta debe bastar –apdo. III–. Además, afirma que la LAECSP «debe proclamar y erigirse sobre un principio fundamental como es la conservación de las garantías constitucionales y legales a los derechos de los ciudadanos y, en general, de las personas que se relacionan con la Administración Pública cuya exigencia se deriva del artículo 18.4 de la CE, al encomendar a la Ley la limitación del uso de la informática para preservar el ejercicio de los derechos constitucionales. Esta conservación exige afirmar la vigencia de los derechos fundamentales no sólo como límite, sino como vector que orienta la reforma legislativa de acuerdo con el fin promocional consagrado en el artículo 9.2 de nuestro texto fundamental, así como recoger aquellas peculiaridades que exigen la aplicación segura de estas tecnologías» –apdo. V–(51). Se habla así de la existencia de un «Estatuto del ciudadano frente a la Administración electrónica».

Así, la LAECSP establece como principio general que regula la utilización de las tecnologías de la información y la comunicación en la Admi-

---

efectos de requerir información, si procediera–; ejercicio de los derechos de acceso, rectificación, cancelación u oposición –si existían formularios para el ejercicio de los mismos; procedimiento para el ejercicio de estos derechos–. También se hicieron requerimientos relativos al deber de secreto, al cumplimiento del art. 12 de la LOPD y a la implantación de medidas de seguridad. Estas inspecciones finalizaron con una Instrucción del Director de la Agencia de Protección de Datos de la Comunidad de Madrid en la que se determinaba el grado de cumplimiento de la normativa de protección de datos, estableciendo las medidas que, en cada caso, era necesario poner en práctica para la adecuación a los principios y derechos establecidos en la LOPD.

(51) Así el Real Decreto 1671/2009, de 6 de noviembre, establece como uno de sus principios estratégicos la garantía de que en el desarrollo de los servicios de Administración electrónica no resultan afectados otros bienes constitucionalmente protegidos, como pueden ser la protección de datos, los derechos de acceso a la información administrativa o la preservación de intereses de terceros –Exposición de Motivos–.

nistración Pública «el respeto al derecho a la protección de datos personales en los términos establecidos en la LOPD, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar» –art. 4.a)–. También hay que destacar el reconocimiento de un principio de seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas –art. 4.f)–. De hecho, la LAECSP reconoce como un derecho de los ciudadanos «la garantía de la seguridad y la confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas» –art. 6.2.i)–. Esto significa el cumplimiento de los principios de protección de datos, especialmente como señala el Grupo de Trabajo del Artículo 29, los relativos a la calidad de los datos, la legitimidad del tratamiento y la información a las personas afectadas, así como al nivel de seguridad aplicable, cuestiones que analizaremos seguidamente. Una vulneración de los principios y derechos de protección de datos en el ámbito de la Administración electrónica puede conllevar la nulidad o la anulabilidad del acto administrativo –arts. 62.1 y 63 LRJAP–(52).

3. LAS TECNOLOGÍAS DE PROTECCIÓN DEL DERECHO A LA INTIMIDAD Y LA PRIVACY BY DESIGN

La voluntad de mejorar la protección de los datos personales en el ámbito de las tecnologías de la información y las comunicaciones aconseja alcanzar algunas sinergias con la industria de las TIC, para tratar de que los equipos informáticos y el *software* estén fabricados de una manera que permita el control de los propios datos personales(53). En esta dirección, la Disposición Adicional Única del Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre señala que «los productos de *software* destinados al tratamiento automati-

(52) Esta cuestión ha sido analizada por M. Fernández Salmerón, *La protección de los datos personales en las Administraciones Públicas*, cit., pp. 465 a 470. Lógicamente, la nulidad del acto administrativo se produce si existe una violación del derecho fundamental a la protección de datos, lo que no viene derivado de cualquier incumplimiento de la normativa de protección de datos personales –por ejemplo, de la ausencia de la declaración del fichero y de su inscripción en el registro general– sino de la vulneración de los principios y derechos que conforman su contenido esencial. Cfr. más ampliamente A. Troncoso Reigada, «La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional», *Cuadernos de Derecho Público,* núms. 19-20, 2003 pp. 231-334.

(53) Muchas amenazas al derecho fundamental a la protección de datos personales provienen directamente de las tecnologías de la información –de los equipos informáticos y de los programas de *software*– y de los protocolos de comunicaciones y transmisión de datos. Por ello, se hace necesario desarrollar sistemas operativos que dificulten las operaciones que puedan suponer vulneraciones del derecho a la protección de datos personales –evitando, por ejemplo, la introducción de programas espías y otros dispositivos ocultos en el equipo terminal del usuario– y que reduzcan al mínimo el tratamiento de datos personales. Cfr. A. Sánchez Navarro, *loc. cit.*, p. 100.

zado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento». Esta previsión ofrece al ciudadano la posibilidad de conocer el grado de cumplimiento de las medidas de seguridad que tiene cada producto –lo que le facilita el control de la propia información personal–, y promueve que los productos de *software* destinados al tratamiento de datos personales cumplan las medidas de seguridad(54). Ésta es una cuestión a la que se ha referido la Directiva 2002/58/CE, de 12 de julio de 2002 del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas –art. 14.3–, que establece que «cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales»(55). En esta dirección, se ha planteado la necesidad de construir unas tecnologías de protección del derecho a la intimidad (PET) que pueden ser definidas como «un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información»(56). Si bien la tecnología no basta

---

(54) Esta previsión fue impugnada ante el Tribunal Supremo por la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) que la desestimó. La Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de julio de 2010 –Sección Sexta–, en el Fundamento Jurídico Vigesimotercero señala que esta disposición adicional «no impone a los responsables y encargados de los ficheros y tratamientos la utilización de un producto de determinadas características, en cuanto que lo único que exige es que se describan las características técnicas del producto para que el adquirente pueda conocer si el nivel de seguridad que ofrecen cumple con las medidas que de tal naturaleza se previenen en el Título VIII, relativo a las medidas de seguridad en el tratamiento de datos de carácter personal, ni implica una restricción al comercio, pues dentro del ámbito competencial que le es propio, lo único que viene a exigir, en garantía de los compradores y también de los afectados por el tratamiento de datos, es la indicación de aquellas características. En definitiva, responde a los deberes de seguridad que impone el artículo 9 de la Ley».

(55) El Considerando 46 afirma que «puede resultar necesario adoptar medidas que exijan a los fabricantes de determinados tipos de equipos utilizados en los servicios de comunicaciones electrónicas que fabriquen sus equipos de manera que incorporen salvaguardias para garantizar la protección de los datos personales y la intimidad del usuario y el abonado».

(56) Cfr. también la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) –COM (2007) 228 final–, de 2 mayo 2007. Este documento está disponible en *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:ES:PDF*. La Comisión toma esta definición de las PET del Proyecto Pisa que financia la Unión Europea. Para la Comisión el régimen normativo de la Directiva y de las legislaciones nacionales puede resultar insuficiente cuando los datos personales se difunden por todo el mundo a través de las redes de TIC y en su tratamiento intervienen varias jurisdicciones, a menudo fuera de la UE. Para la Comisión, si bien «la responsabilidad jurídica del cumplimiento de las normas de protección de datos personales recae en los responsables de su tratamiento, desde el punto de vista social y ético también recae en

por sí sola para proteger la intimidad, se ha afirmado la necesidad de fomentar las aproximaciones tecnológicas que proporcionen herramientas necesarias para el cumplimiento de la legislación de protección de datos personales(57).

---

parte, por ejemplo, en quienes elaboran las especificaciones técnicas y quienes realmente desarrollan o ejecutan programas o sistemas operativos». Por ello, la Comisión entiende que es necesaria la utilización de las tecnologías para favorecer el cumplimiento de la legislación, en particular las normas de protección de datos. Así, «gracias a dichas tecnologías, las infracciones de las normas de protección de datos y la vulneración de los derechos del ciudadano, además de estar prohibidas y sujetas a sanciones, resultarían más difíciles desde el punto de vista técnico». Esta Comunicación de la Comisión es consecuencia del Primer informe sobre la aplicación de la Directiva sobre protección de datos y enlaza con la Comunicación de la Comisión «Una estrategia para una sociedad de la información segura» [COM (2006) 251, de 31 de mayo de 2006], donde se invitaba al sector privado a «estimular el despliegue de productos, procesos y servicios que favorezcan la seguridad a fin de evitar y combatir la sustracción de la identidad y otros ataques contra la privacidad». Con esta comunicación, la Comisión trata de fomentar la utilización de las PET por parte de los responsables del tratamiento de datos y los consumidores. Afirma la necesidad de la configuración de grupos –entre los que deben incluirse las autoridades de protección de datos– que se encarguen de analizar la evolución de la tecnología, detectar los peligros que plantea en relación con los derechos fundamentales y la protección de datos personales y definir los requisitos técnicos para hacerles frente. Hay que destacar que la Comunicación de la Comisión destaca la necesidad de fomentar el uso de las PET por parte de las Administraciones Públicas, siguiendo en este punto Comunicación de la Comisión sobre el papel de la administración electrónica en el futuro de Europa –COM (2003) 567 final, de 26 septiembre 2003–. La Administración electrónica debe emplear PET con objeto de generar la confianza necesaria para funcionar de forma satisfactoria: «La Comisión invita a los Gobiernos a que garanticen la protección de datos en los programas de Administración electrónica, entre otras cosas recurriendo en la mayor medida posible a las PET en el diseño y aplicación de los mismos». Este Comunicado de la Comisión al Parlamento sobre el fomento de las tecnologías de la información cita también el *Proyecto PRIME («Privacy and Identity Management in Europe»)*, que tiene como objetivo construir un conjunto de herramientas informáticas que ayuden a los usuarios de Internet a mantener bajo su control la información que revelan de sí mismos mediante una gestión de identidad que hace un énfasis especial en la protección de la privacidad. Quisiera destacar que la Agencia de Protección de Datos de la Comunidad de Madrid ha colaborado en la elaboración de un libro blanco y la aportación de ideas para los prototipos que se han construido para aplicar las ideas del proyecto. También quisiera mencionar la participación de la Agencia en el proyecto *«Breaking Barriers to Electronic Government»*, que coordina la Universidad de Oxford, acerca de las dificultades para la expansión de la Administración Electrónica y las necesarias iniciativas a nivel europeo para eliminarlas. La Agencia finalizó durante el año 2007 el proyecto europeo e-PRODAT sobre *Mejores prácticas en materia de protección de datos en los servicios regionales de e-Administración*, a cuya publicación se ha hecho mención con anterioridad.

(57) Cfr. Y. POULLET –con la colaboración de J.-M. DINANT, «Hacia nuevos principios de protección de datos en un nuevo entorno TIC», *Revista de Internet, Derecho y Política*, nº 5, 2007, editada por la UOC– *http://www.uoc.edu/idp*. Estos autores plantean también el principio de que «los usuarios de determinados sistemas de información deberían beneficiarse de la legislación de protección al consumidor» –p. 33–. Sin embargo, a nuestro juicio, la protección de datos, que como derecho fundamental dispone de todas las garantías genéricas y específicas de protección, no puede abordarse desde la perspectiva de los derechos de los consumidores, que otorga un menor nivel de tutela.

Estas Tecnologías de protección de la privacidad –PET– se enmarcan en un conjunto de iniciativas que tratan de promover el cumplimiento del derecho fundamental a la protección de datos personales a través de medidas positivas que involucren al propio sector, y entre las que hay que destacar también la aprobación de Códigos Tipo –que están previstos en la Directiva 95/46/CE, en la LOPD y que han tenido un impulso en el reciente Reglamento de desarrollo de la LOPD que ha regulado incluso la existencia de autoridades de supervisión y de sanciones–, o la creación de un modelo de certificación de privacidad para productos y servicios(58). De hecho, la Resolución de Estándares Internacionales aprobada en la 31ª Conferencia Internacional sobre Privacidad y Protección de Datos celebrada en Madrid en 2009 ha resaltado la importancia de «la adhesión a acuerdos de autorregulación cuya observancia resulte vinculante, que contengan elementos que permitan medir sus niveles de eficacia en cuanto al cumplimiento y grado de protección de los datos de carácter personal y establezcan medidas efectivas en caso de incumplimiento» –art. 22–(59).

(58) La Agencia de Protección de Datos de la Comunidad de Madrid, junto con las Autoridades de Protección de Datos de Francia (CNIL) y del Länder de Scheswig-Holstein (Alemania) –y otros socios de Reino Unido, Alemania, Austria, Suecia, Eslovaquia y Holanda–, está impulsando el *Proyecto EuroPriSe*, que trata de poner las bases para el establecimiento de un Sello Europeo de Privacidad para productos y servicios de Tecnologías de la Información en los sectores público y privado. Este proyecto se encuentra financiado por la Comisión Europea a través del programa eTEN. *EuroPriSe* se basa en una evaluación del producto o servicio por parte de expertos, tanto jurídicos como de tecnologías de la información y una validación del informe de evaluación por parte de un organismo de certificación independiente. La evaluación y certificación se lleva a cabo conforme a los criterios de la normativa europea de protección de datos. La Comunicación de la Comisión antes citada sobre las PET menciona como una iniciativa muy interesante «un sistema europeo de distintivos de protección de la intimidad, que incluiría asimismo un análisis de las repercusiones económicas y sociales. Gracias a dichos distintivos, los consumidores podrían reconocer fácilmente los productos que cumplen o favorecen el cumplimiento de las normas de protección de datos en el tratamiento de éstos, en concreto mediante la aplicación de PET apropiadas». La Comisión considera que, para que los distintivos cumplieran su objetivo, habrían de respetarse los principios siguientes: «El número de sistemas de distintivos debería reducirse al mínimo, pues la proliferación de distintivos podría crear mayor confusión al consumidor y mermar su confianza en todos los distintivos; de ahí la pertinencia de valorar si sería preciso integrar –y en qué medida– un distintivo europeo de protección de la intimidad en un sistema más general de certificación de seguridad. –Los distintivos deberían concederse únicamente a los productos que cumplan una serie de reglas que corresponden a las normas de protección de datos. Las reglas deberían ser tan uniformes como fuera posible en toda la UE–. Las autoridades públicas, en particular las autoridades nacionales responsables de la protección de datos personales, deberían desempeñar un papel importante en el sistema participando en la definición de reglas y procedimientos pertinentes, y en la supervisión del funcionamiento del mismo».

(59) Esta es una cuestión que hemos analizado en el estudio «La necesidad de unos estándares internacionales de protección de datos personales y las posibilidades que brinda la autorregulación a este respecto», que se publicará dentro de las *Actas a la 31ª Conferencia Internacional sobre Privacidad y Protección de Datos.*

Dentro de este marco hay que incluir también la *privacy by design*, que tiene la virtualidad de situar el análisis de la privacidad en el momento del diseño de las aplicaciones informáticas. Con carácter previo a la implantación de un servicio de Administración electrónica es necesario analizar cómo van a cumplirse las obligaciones establecidas en la legislación de protección de datos personales. Por tanto, hay que introducir en la metodología de la configuración del sistema de información para la Administración electrónica las evaluaciones de impacto en la privacidad –las *privacy impact assesment*–. Así, como señalaremos más adelante, es necesario que antes de establecer un modelo de interconexiones de sistemas de información exista un informe preceptivo de las Autoridades de control que valoren la adecuación, necesidad y proporcionalidad de esta injerencia en el derecho fundamental a la protección de datos personales. La *privacy by design* supone una respuesta al riesgo, que acertadamente destaca VALERO TORRIJOS, de que «las aplicaciones informáticas acaben por condicionar el ejercicio competencial de manera que los órganos administrativos a quienes corresponde dicha función sean suplantados por los programadores» de empresas privadas o de las propias Administraciones Públicas(60).

4. LA DECLARACIÓN DE FICHEROS Y TRATAMIENTOS DE DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA Y LA FUNCIÓN DEL RESPONSABLE

La LOPD exige que los ficheros y tratamientos de datos personales de las Administraciones Públicas sean declarados a través de una disposición de carácter general e inscritos en un registro de ficheros –art. 20 LOPD–(61), unas garantías necesarias para ejercer el derecho de consulta –art. 14 LOPD–. La LOPD define como responsable del fichero o tratamiento a la persona que decide sobre la finalidad, contenido y uso del tratamiento –art. 3.d) LOPD–(62), algo que no siempre es fácil de determinar en cada caso concreto(63). El responsable del fichero en el

(60) Cfr. J. VALERO TORRIJOS, «Acceso a los servicios y difusión de la información por medios electrónicos», en E. GAMERO CASADO y J. VALERO TORRIJOS (Coord.), *La Ley de Administración Electrónica*, cit., p. 270.

(61) No olvidemos que el artículo de la 44.3.a) de la LOPD establece como infracción grave la de proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos sin autorización de disposición general, publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente –no modificado por la Ley 2/2011, de 4 de marzo–.

(62) El art. 5.1.q) del Reglamento de desarrollo de la LOPD define como responsable al órgano administrativo que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realice materialmente –y se apoye en un encargado–.

(63) La determinación del responsable del fichero es una cuestión que hemos analizado en «La huida de la Administración Pública hacia el Derecho privado y la privatización de los servicios públicos: consecuencias en el régimen jurídico de los ficheros de datos personales y en la delimitación del responsable y del encargado del tratamiento», *Anuario de la Facultad de Derecho de la Universidad de Alcalá de Henares*, 2009, pp. 59-71.

ámbito de las Administraciones Públicas –y dentro del régimen jurídico de los ficheros públicos– es aquel que decide la puesta en marcha y la finalidad del servicio de Administración electrónica y tiene la competencia administrativa para la cual el tratamiento de datos personales es instrumental(64). La LAECSP establece que las disposiciones de creación de registros electrónicos se publicarán en el Diario Oficial correspondiente y especificarán el órgano o unidad responsable de su gestión –art. 25.1–(65). Este órgano tendrá a los efectos de la LOPD el carácter de responsable del fichero del registro electrónico para la recepción o salida de las solicitudes, escritos y comunicaciones, con independencia de cuál sea el órgano administrativo competente para la tramitación efectiva del procedimiento que se inicie, sea la tramitación electrónica o no(66). El tratamiento de datos del que es responsable el titular del registro electrónico consistirá únicamente en facilitar la recepción de las solicitudes planteadas por los ciudadanos, sin acceder a su contenido, dando traslado de las mismas al órgano competente para el inicio y tramitación del procedimiento. Si posteriormente todo el procedimiento administrativo se tramita de manera electrónica, dichos procedimientos pueden igualmente precisar de la declaración del correspondiente fichero informático donde se va a proceder a los tratamientos de datos personales relativos a ese procedimiento –el expediente electrónico–(67), siendo responsable del fichero el órgano que tuviera la competencia para su resolución. Algo semejante puede decirse cuando se opta por una tramitación parcial del procedimiento por medios electrónicos –imprimiendo parte de la documentación en papel, lo que supone un fichero o tratamiento parcialmente automatizado–. También debe ser declarado a través de una disposición de carácter general e inscrito en el registro el fichero del repositorio de datos o documentales, cuyo responsable será el órgano administrativo al que se le encomiende la gestión del repositorio, tal

(64) El art. 15.2 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid señala que se entenderá por responsable del fichero «el órgano titular de la función específica en que se concrete la competencia material a cuyo ejercicio sirva instrumentalmente el fichero».

(65) Ha desaparecido la previsión del art. 45.4 de la LRJ-PAC, que establecía que «los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características». El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, establece que por «orden del Ministro de la Presidencia se establecerán los requisitos y condiciones de funcionamiento del Registro Electrónico Común, incluyendo la creación de un fichero ajustado a las previsiones de la normativa sobre protección de datos de carácter personal» –art. 31–.

(66) El fichero del registro electrónico de documentos sirven también para almacenar comunicaciones de los ciudadanos que no se ajustan exactamente a ningún procedimiento administrativo concreto ni a un fichero de atención al ciudadano, sugerencias o reclamaciones.

(67) Este tratamiento automatizado de datos personales consistiría en el inicio, seguimiento y resolución de las solicitudes de los ciudadanos.

como se especifique en la disposición general de establecimiento del servicio. Si no existe tal órgano, cada órgano administrativo sería el responsable de su documentación administrativa(68). Normalmente, el responsable del fichero de *cookies* no es el órgano administrativo competente sobre cada información administrativa sino el órgano responsable de la estructura de comunicación en Internet de la Administración Pública(69).

No obstante, los datos personales recabados por medios electrónicos también pueden considerarse incluidos en alguno de los ficheros preexistentes ya declarados por la Administración para la misma finalidad, modificando en su caso el anexo relativo a la «procedencia de los datos y procedimiento de recogida». Así, el fichero del registro de entrada se encuentra frecuentemente ya declarado, siendo necesaria una modificación de la declaración para adecuar el sistema de información(70). Algo semejante ocurre en el caso de muchos procedimientos administrativos o del DNI-e. Este último es un fichero informatizado de datos personales

(68) El Real Decreto 1671/2009, de 6 de noviembre, prevé la existencia de un registro electrónico de apoderamientos para actuar electrónicamente ante la Administración General del Estado y sus organismos públicos dependientes o vinculados, estableciendo que el Ministerio de la Presidencia creará los ficheros de datos personales necesarios y gestionará dicho registro, que deberá coordinarse con cualquier otro similar existente de ámbito más limitado en la Administración General del Estado –art. 15.2–.

(69) Debe existir un fichero de la web institucional para la función de comunicación y donde se incorporarían el tratamiento de datos personales relativos a las *cookies* u otros tratamientos de datos derivados del portal de la Administración. Así, por ejemplo, en el ámbito de la Comunidad de Madrid hay que señalar que el art. 10 de la Ley 7/2005, de 23 de diciembre, de medidas fiscales y administrativas, en el que se definen las funciones del Ente público Agencia de Informática y Comunicaciones de la Comunidad de Madrid, se destacan las siguientes: «c) La prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid, mediante medios propios o ajenos, a cuyo fin le corresponde particularmente: 1. La administración, mantenimiento y soporte de los equipos físicos y lógicos de tratamiento de la información y de las comunicaciones de cualquier especie que se encuentren instalados en la misma. 2. El desarrollo y adquisición de aplicaciones informáticas y sistemas de información para la Comunidad de Madrid, y su mantenimiento y soporte posteriores, de acuerdo con las especificaciones funcionales y necesidades de los distintos centros directivos. 3. La adquisición y dotación de infraestructuras físicas y lógicas de soporte de los sistemas de información y comunicaciones de la Comunidad de Madrid, y de sus servicios. d) El establecimiento de las características técnicas exigibles al equipo físico y lógico de tratamiento de la información y de las comunicaciones desarrollados o adquiridos por la Comunidad de Madrid y el control del cumplimiento de la normativa a que deberán atenerse, a fin de asegurar su utilidad y compatibilidad. i) La elaboración de la normativa e instrucciones para la utilización de los diferentes equipamientos por los usuarios. j) La seguridad, confidencialidad, integridad y disponibilidad de la información tratada, en su ámbito de responsabilidad».

(70) La implantación de la Administración electrónica obliga a modificar la declaración, por ejemplo, cuando se amplía la tipología de datos o cuando se establecen los medios electrónicos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. En cambio, no sería necesario modificar la declaración cuando se añade la dirección electrónica a los datos de contacto con los ciudadanos.

que debe estar ya declarado a través de una disposición de carácter general(71). Como hemos señalado anteriormente, tanto la publicación de información administrativa en Internet como la edición electrónica de un Boletín o Diario Oficial constituyen claros ejemplos de ficheros o tratamientos de datos de carácter personal de titularidad pública, que deben estar declarados a través de una disposición de carácter general e inscritos en el registro de ficheros. Hemos analizado en otro momento las dificultades que supone la determinación de la figura del responsable del fichero entre el órgano administrativo que ordena la inserción de la información administrativa y aquel que tienen la competencia administrativa de publicar el diario oficial o de gestionar la web institucional(72). Únicamente quisiéramos destacar ahora que el desarrollo y la gestión de las páginas web de las Administraciones Públicas tanto para mejorar la información que se ofrece a los ciudadanos como para prestar servicios públicos pueden estar encomendados a otras Administraciones –es el caso de Ayuntamientos pequeños que se lo encargan a una Diputación Provincial o a una Comunidad Autónoma uniprovincial– o a empresas privadas que actúan como proveedoras de servicios de Internet o gestionan las aplicaciones informáticas para la mecanización de los procedimientos administrativos. Estas se constituyen en encargados del tratamiento y deben cumplir los requisitos establecidos en el art. 12 de la LOPD(73). El responsable del tratamiento de los datos personales que pueden volcarse en dichas webs sigue siendo la Administración que tiene la competencia administrativa y que decide sobre finalidad, contenido y uso del mismo –que tiene también que garantizar los derechos de acceso, rectificación, cancelación y oposición y responder de las posibles infracciones–, con independencia de quién gestione materialmente los ficheros o proporcione las aplicaciones informáticas.

Por tanto, el responsable del fichero –que es el que tiene la competencia administrativa para la cual el tratamiento de datos personales es

---

(71) De hecho, la Disposición final segunda del Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del DNI y sus certificados de firma electrónica obliga al Ministerio del Interior a adoptar las disposiciones necesarias para dar cumplimiento a lo previsto en la LOPD, en materia de creación y modificación de ficheros de titularidad pública. El responsable del fichero sería la Dirección General de Policía.

(72) No queremos repetir aquí lo ya analizado en otro momento. Nos remitimos por ello a «Transparencia administrativa y protección de datos personales», cit., pp. 101-112.

(73) Como hemos señalado en otro momento, la figura del encargado del tratamiento exige que el acceso a los datos se produzca *por cuenta de terceros* –art. 12 LOPD– por lo que no puede hablarse de que un departamento administrativo actúa como encargado del tratamiento de otro dentro de la misma Administración Pública. De esta forma, la unidad administrativa responsable de la edición electrónica del boletín oficial o del sitio web institucional en Internet no es una encargada del tratamiento de datos por cuenta del responsable del fichero –tampoco un cesionario–, sino que se trata de accesos vinculados al principio de finalidad. Cfr. «El principio de calidad de los datos», en A. Troncoso Reigada, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, cit., pp. 382-394.

instrumental– está obligado a implantar el servicio de Administración electrónica respetando el cumplimiento de los principios y derechos reconocidos en la LOPD. El responsable administrativo que decide la recogida de datos personales tiene que valorar qué datos personales va a recoger y para qué finalidad, quién puede acceder a la información dentro de la organización, cómo va a garantizar el principio de información en la recogida de datos y el consentimiento para el tratamiento en las cesiones y en los servicios de valor añadido, cómo va a implantar las medidas de seguridad y cómo garantizará el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, siendo consciente de que ser responsable de un fichero y tratamiento implica asumir la responsabilidad de las posibles infracciones derivadas del incumplimiento de la legislación. De alguna manera –profundizando y matizando lo que hemos señalado anteriormente–, la protección de datos personales supone en un primer momento un límite a la Administración electrónica(74). Sin embargo, el responsable administrativo no tiene otra opción que adecuar los tratamientos de datos personales en el servicio de Administración electrónica a los principios y derechos de protección de datos. Aunque existan posibilidades técnicas para que los ciudadanos puedan ejercer sus derechos del art. 6 LAECSP ante la Administración por medios electrónicos, esta implantación se encuentra supeditada a que también se cumpla la normativa de protección de datos personales. De lo contrario, como señala VALERO TORRIJOS, «podríamos encontrarnos con la paradoja de que la satisfacción de tales derechos supondría la vulneración de otro, en este caso incluso con el máximo rango constitucional al tratarse de un derecho fundamental»(75).

III. EL PRINCIPIO DE CALIDAD EN LA ADMINISTRACIÓN ELECTRÓNICA

1. EL PRINCIPIO DE FINALIDAD Y EL ACCESO POR LOS DEPARTAMENTOS DE LA MISMA ADMINISTRACIÓN

La Administración Electrónica tiene que tener en cuenta especialmente el principio de calidad –art. 4 LOPD–. Es muy importante que los datos sólo se utilicen para la finalidad para la cual han sido recabados y no para finalidades incompatibles –art. 4.2 LOPD–. Aunque los principios de protección de datos, y, en concreto, el principio de finalidad también afecta a los tratamientos de datos personales no automatizados, el hecho

(74) CERRILLO señala que una regulación más flexible de la LOPD «de la cesión de datos entre Administraciones Públicas, la calidad de los datos, su comunicación o los derechos de los ciudadanos en relación a los datos, y, en particular, el derecho de rectificación y cancelación podría facilitar la interoperabilidad». Cfr. A. CERRILLO I MARTÍNEZ, «La interoperabilidad», cit., p. 35.

(75) Cfr. J. VALERO TORRIJOS, «Implicaciones de la protección de datos de carácter personal para la Administración electrónica», cit., p. 180.

de que los datos personales derivados de la propia tramitación administrativa vayan a ser objeto de tratamiento y almacenamiento en ficheros informáticos permite potencialmente cruzar y relacionar esa información personal. Como señala la Exposición de Motivos de la LAECSP, «la progresiva utilización de medios electrónicos suscita la cuestión de la privacidad de unos datos que se facilitan en relación con un expediente concreto pero que, archivados de forma electrónica como consecuencia de su propio modo de transmisión, hacen emerger el problema de su uso no en el mismo expediente en el que es evidente, desde luego, pero sí la eventualidad de su uso por otros servicios o dependencias de la Administración o de cualquier Administración o en otro expediente» –apdo. III–. Pues bien, los datos personales aportados por un ciudadano al iniciar un procedimiento administrativo o los que se obtengan posteriormente deben estar vinculados a éste y no pueden ser empleados por otros departamentos administrativos en otros procedimientos(76). De esta forma, el tratamiento de los datos para otra finalidad sólo será legítimo en virtud de una habilitación legal que establezca claramente la competencia administrativa para tratar esa información(77). Sin embargo, no siempre es suficiente que el segundo tratamiento entre dentro de las competencias legales del órgano administrativo. Lógicamente, es necesario ser muy estricto en el respeto al principio de finalidad en la información aportada voluntariamente por el interesado. En este último caso el tratamiento de los datos para finalidades distintas –sobre todo cuando pueden suponer una valoración de determinados aspectos de la personalidad que le pueda perjudicar de manera significativa– requiere el consentimiento del interesado ya que posiblemente para este segundo supuesto el interesado no hubiera ofrecido voluntariamente esta información. Además, el art. 4.7 de la LOPD «prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos», lo que veda los tratamientos ocultos –como las *cookies*– si no existe información y consentimiento del interesado.

Es necesario resaltar que cada Administración Pública es una personalidad jurídica única –art. 3.4 LRJAP y PAC– por lo que los accesos de

(76) Así, por ejemplo, vulneraría el principio de finalidad que en los registros electrónicos se llevara a cabo un tratamiento de datos personales que vaya más allá de la puesta a disposición de la información al órgano en que resida la competencia para la tramitación del expediente administrativo o del servicio solicitado por el interesado. Cfr. la Recomendación 3/2008 de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica.

(77) En otro momento hemos analizado la problemática de las finalidades distintas y de las finalidades incompatibles, una cuestión sobre la que ha sido restrictiva la jurisprudencia de la Audiencia Nacional, en contradicción con el tenor literal del art. 4.2 de la LOPD. La compatibilidad de la finalidad en el ámbito de los ficheros públicos tiene mucho que ver con la competencia administrativa cuando ésta tenga suficiente cobertura legal. Así, a nuestro juicio, la Administración puede utilizar los datos para finalidades que, en principio, pudieran parecer distintas a las que figuran en la declaración del fichero, pero que son compatibles y adecuadas a la competencia administrativa del órgano que recoge los datos, siempre que se cumplan una serie de requisitos que hemos analizado en otro momento. Cfr. A. TRONCOSO REIGADA, «El princi-

los distintos departamentos están sometidos al principio de finalidad, no tratándose de una cesión de datos personales. Así, en muchas ocasiones, el cumplimiento de la finalidad del fichero implica que distintos departamentos de la misma Administración Pública deban acceder a la información personal. En otras ocasiones, si bien este acceso no respeta la finalidad inicial del tratamiento, existe una habilitación legal –o una competencia administrativa de otro órgano que dispone de una adecuada cobertura legal–(78). A diferencia del art. 35.f) de la LRJAP que establecía el derecho de los ciudadanos «a no presentar documentos no exigidos por las normas aplicables al procedimiento de que se trate, o que ya se encuentren en poder de la Administración actuante», la LAECSP reconoce a los ciudadanos el derecho a «no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información» –art. 6.2.b)–. Este planteamiento, además de tener implicaciones en lo relativo a las comunicaciones entre Administraciones Públicas –como después analizaremos–, obliga a facilitar los accesos a documentos en el marco de la misma Administración Pública, aunque las competencias se encuentren atribuidas a distintos Ministerios, Consejerías o Concejalías. Lógicamente el ejercicio por parte del ciudadano de su derecho a no aportar datos que obren en poder de la Administración supone el consentimiento del interesado para la utilización de sus datos personales para una finalidad distinta, lo que incluye el acceso a aquellos datos incorporados a repositorios.

El respeto al principio de finalidad en el ámbito de la Administración electrónica exige ser muy estrictos en la definición de las personas que tienen permiso para acceder a la información de manera que no todo el personal pueda acceder a los datos personales sometidos a tratamiento en un servicio de Administración electrónica –por ejemplo, una historia clínica electrónica– sino únicamente aquellas personas que necesiten acceder a la información para el cumplimiento de sus funciones –los facultativos que prestan la asistencia pero no aquellos que no la prestan o han dejado de prestarla, tampoco el personal de administración y servicios salvo aquella información indispensable para el cumplimiento de sus funciones–. La Administración electrónica aporta en este punto herramientas que permiten implementar estos diferentes niveles de acceso a la información administrativa, algo que es muy complejo de materializar en los tratamientos de datos en papel.

2. EL PRINCIPIO DE ADECUACIÓN Y PROHIBICIÓN DE EXCESO

El principio de calidad establece también que sólo se traten aquellos datos que sean adecuados y pertinentes para esa finalidad, no debiéndose

---

pio de calidad de los datos», cit., pp. 366-370.

(78) Sobre los accesos a un fichero por parte de departamentos de la misma Administración, cfr. *ibídem*, pp. 382-394.

almacenar en ningún caso datos excesivos –art. 4.1 LOPD–. Si las tecnologías de la información permiten potencialmente una acumulación masiva de información personal, hay que analizar cuidadosamente qué datos se piden y para qué finalidad, qué datos se almacenan y qué datos se cancelan(79). El respeto al principio de adecuación y de prohibición de exceso es especialmente importante en el ámbito de la Administración electrónica, que en muchas ocasiones lleva a cabo tratamientos de datos personales sin consentimiento del interesado –art. 6.2 LOPD– en virtud de una habilitación legal, para el cumplimiento de funciones administrativas o por ser requeridos para dar cumplimento a una relación administrativa, por ejemplo, para recibir una prestación social que el interesado solicita(80). La LAECSP proclama un principio de proporcionalidad, por el que «sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten» –art. 4.g)–. De hecho, el respeto al principio de adecuación, pertinencia y prohibición de exceso en el tratamiento de datos personales es una garantía adicional del sometimiento al principio de finalidad(81) y es especialmente aplicable a los accesos y cesiones de datos personales dentro de los servicios de Administración electrónica(82). Así, como señalaremos

(79) Así, por ejemplo, es importante que en los instrumentos de participación social y en los foros de discusión dentro de los sitios web institucionales de la Administración Pública se recojan únicamente los datos personales estrictamente necesarios –por ejemplo, el correo electrónico– para poder participar y opinar en dichos foros, no dando publicidad a esa información personal si no es con el consentimiento del interesado. Lo ideal sería no recoger ninguna información personal ya que su vinculación a una opinión puede suponer un tratamiento de datos de ideología, lo que exige el consentimiento expreso y escrito –con expresa advertencia del derecho a no prestarlo– y la implantación de medidas de seguridad de nivel alto. Además, la información facilitada por las personas no debe ser utilizada para fines distintos a los de la propia participación y debe ser cancelada cuando haya dejado de ser necesaria. Si bien las opiniones vertidas por los ciudadanos se encuentran protegidas por la libertad de expresión del art. 20.1ª), puede ser considerado contrario al principio de calidad aquellos comentarios que menoscaben el derecho al honor y a la intimidad de otras personas. Estos datos deben ser suprimidos por el Administrador del foro. De hecho, si éste no cancela estos comentarios indebidos, teniendo la capacidad para decidir sobre el mantenimiento o no de la publicación de esa información, debe considerarse responsable –para eso es el responsable del tratamiento aunque el origen de los datos provenga de terceras personas–. Cfr. en esta dirección L. De Salvador Carrasco, «Retos de la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos», cit.

(80) Es especialmente importante el respeto al principio de adecuación y prohibición de exceso en la elaboración por parte de la Administración de los formularios con formato preestablecido.

(81) El documento de trabajo del Grupo del Artículo 29 sobre la Administración en línea ya mencionado señala que para satisfacer la condición de la recogida leal de datos, la Autoridad irlandesa recomienda no alimentar la base de datos con información facilitada para un fin distinto. Asimismo, este documento de trabajo pone énfasis en la importancia de no exigir ni conservar datos personales excesivos porque no tendrán una aplicación legítima y pertinente para la eficacia del servicio público.

(82) Es muy importante que la publicación de información administrativa con datos personales en los servicios de Administración electrónica –edición electrónica de diarios oficiales, publicación de actos administrativos o de sesiones en los sitios web

más adelante, la LAECSP establece, en relación con la transmisión de datos entre Administraciones Públicas, que la disponibilidad de tales datos «estará *limitada estrictamente* a aquellos que son requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos» –art. 9.2–. Así, sólo se van a transmitir los datos exigidos por la normativa y únicamente en el ámbito de un procedimiento concreto y a la Administración competente. Estos principios de adecuación y prohibición de exceso deben estar muy presentes en los tratamientos de datos especialmente protegidos por los servicios de Administración electrónica(83).

El principio de calidad obliga a almacenar los datos «de forma que permitan el ejercicio del derecho de acceso» –art. 6 LOPD–. La Administración electrónica, como señalaremos más adelante, facilita el ejercicio pleno de este derecho. Hay que recordar que el derecho de acceso faculta para conocer el origen de los datos sometidos a tratamiento y las comunicaciones realizadas y que se prevén en el futuro. Por ello, debe conservarse la trazabilidad del origen de los distintos datos –facilitados por el propio interesado, generados por los actos de trámite o resolutorios del procedimiento, otras fuentes, etc.– y de su destino. Por otra parte, la Administración electrónica ayuda al almacenamiento de información personal. La LAECSP reconoce a los ciudadanos el derecho a la «conservación en formato electrónico por las Administraciones Públicas de los do-

---

institucionales– se limite a aquellos datos personales de los afectados que resulten imprescindibles para dar cumplimiento al interés público, evitando en todo momento la publicación de datos personales innecesarios para dicha finalidad. Esta es una cuestión que hemos analizado en «Transparencia administrativa y protección de datos personales», cit., pp. 67-74.

(83) El responsable administrativo que ordena la publicación de datos personales debe atender especialmente a la naturaleza de la información tratada, teniendo en cuenta que la distinta tipología de los datos influye en la mayor o menor necesidad de garantizar la confidencialidad de la información. Así, en el caso de los datos especialmente protegidos es importante estar a lo previsto en el art. 61 de la LRJ-PAC que obliga, cuando la publicación del acto pueda lesionar derechos o intereses legítimos, a publicar una somera indicación del contenido del mismo y del lugar físico o electrónico donde los interesados pueden comparecer, en el plazo que se establezca, para el conocimiento íntegro de dichos actos y constancia de tal conocimiento. Esto ocurre, en muchas ocasiones, en las notificaciones de procedimientos administrativos sancionadores o de responsabilidad patrimonial. El cumplimiento del principio de calidad obliga en este caso a que la publicación se limite a la indicación de las iniciales del nombre y de los apellidos, número de Documento Nacional de Identidad y número del expediente administrativo, no debiendo procederse a la publicación de otros datos personales, salvo que exista una previsión legal expresa que obligue a publicar esa información –nombre y apellidos de los sancionados, DNI, infracción cometida y sanción impuesta– y siempre y cuando la sanción sea firme en vía jurisdiccional, no siendo suficiente la existencia de una previsión reglamentaria o que una resolución administrativa prevea esta publicación. Téngase en cuenta que el art. 37.3 de la LRJ-PAC establece que el acceso a los documentos de carácter sancionador o disciplinario se encuentra limitado a la persona del interesado, no pudiendo acceder a dichos datos terceras personas –cfr. *ibídem,* pp. 75-86–.

cumentos electrónicos que formen parte de un expediente» –art. 6.2.f)–. Igualmente, el art. 31.1 de la LAECSP establece que, una vez terminado el procedimiento, «podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas»(84).

3. EL PRINCIPIO DE EXACTITUD Y LA ACTUALIZACIÓN DE LA INFORMACIÓN

El principio de calidad también exige que los datos de carácter personal sean «exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado» –art. 4.3 LOPD–. Es muy importante la exactitud de la información que se maneja en la Administración electrónica porque en muchas ocasiones la vulneración de derechos es ocasionada no por estar en un fichero sino por no estar o por figurar con una información inexacta(85). Cuando de los datos recogidos en la solicitud de un servicio de Administración electrónica o de la comprobación de los mismos se detecte la inexactitud de cualquier información almacenada en el fichero que soporte el servicio, hay que proceder a su corrección. Hay que tener en cuenta que los datos personales que obran en los registros electrónicos, en los repositorios y en las notificaciones electrónicas tienen efectos jurídicos en los derechos de los ciudadanos. Por ello, la LAECSP establece un principio de «responsabilidad y calidad en la veracidad y autenticidad de las informaciones y servicios ofrecidos por las Administraciones Públicas a través de medios electrónicos» –art. 4.h)–. Así, por ejemplo, la LAECSP señala que «el establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma» –art. 10.2–. En relación con el sistema de notificación, la LAECSP señala que éste tiene que permitir «*acreditar* la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso a su contenido, momento a partir del cual la notificación se entenderá practicada a todos los efectos legales» –art. 28.1–. Producirá «los efectos propios de la notificación por comparecencia el acceso electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia de dicho acceso» –art. 28.2–(86). Igual-

(84) El almacenamiento de documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deben conservarse en soportes de esta naturaleza o en cualquiera otro que asegure la integridad de la información –art. 31.2 LAECSP–.

(85) La necesidad de implantar procedimientos de actualización de oficio en los sistemas de información y cómo su ausencia puede lesionar derechos ha sido analizado en «El principio de calidad», cit., pp. 373-374.

(86) El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio permite la práctica de notificaciones en las direcciones de correo electrónico que los ciudadanos elijan «siempre que se genere automáticamente y con independencia de la voluntad del destinatario un acuse de recibo que deje constancia de su recepción y que se origine en el momento del acceso al contenido de la notificación» –art. 39–. Este Real Decreto define la notificación por comparecencia electrónica como el acceso por el interesado, debidamente identifi-

mente, para que las copias de documentos realizadas por medios electrónicos tengan la consideración de copia auténtica con la eficacia prevista en el art. 46 de la LRJAP y PAC, con independencia de cuál fuera su formato original, es necesario que el documento electrónico original se encuentre en poder de la Administración y que la información de firma electrónica y de sellado de tiempo permitan comprobar la coincidencia con dicho documento –art. 30.1–.

Hay que señalar que la Administración electrónica facilita la implantación de procedimientos de oficio para la actualización de la información así como el ejercicio del derecho de rectificación en línea por parte del interesado, lo que permite mantener los datos personales exactos y veraces. También los medios electrónicos contribuyen a la seguridad de la información en el ámbito de la Administración electrónica, lo que garantiza la integridad y la autenticidad de la misma. Más complicado es la aplicación del principio de exactitud en un sistema de Administraciones interconectadas de forma que la información que se mantiene en la red de datos de las Administraciones Públicas sea homogénea(87). Los procedimientos de actualización de la información en un sistema de Administraciones interconectadas tienen que diferenciar que esta actualización provenga del ejercicio del derecho de rectificación y cancelación del ciudadano, de otros supuestos distintos donde la propia interoperabilidad entre Administraciones Públicas sea la causa de la actualización de la información personal. Cuando el ciudadano ha ejercido el derecho de rectificación y cancelación, la actualización de esa información personal en otras Administraciones Públicas proviene de la obligación legal que tiene el responsable, cuando los datos hubieran sido comunicados previamente, de «notificar la rectificación o cancelación efectuada a quien se haya comunicado» –art. 16.4 LOPD–. Sin embargo, hay que ser cuidadoso en la utilización de la interoperabilidad y las interconexiones de datos entre Administraciones Públicas para actualizar la información personal de una Administración a otra. Esta actualización supone una comunicación de datos personales que debe respetar la normativa relativa a las cesiones de datos –que analizaremos posteriormente–, por lo que requiere el cumplimiento de lo previsto en los arts. 11 y 21 de la LOPD, y sobre todo de la existencia de un consentimiento o de una Ley.

---

cado, al contenido de la actuación administrativa correspondiente a través de la sede electrónica del órgano u organismo público actuante –art. 40–. Para que produzca efectos jurídicos de notificación, es necesario que con carácter previo al acceso a su contenido, el interesado pueda visualizar un aviso del carácter de notificación de la actuación administrativa que tendrá dicho acceso. El sistema de información correspondiente dejará constancia de dicho acceso con indicación de fecha y hora.

(87) SALVADOR CARRASCO señala que la LAECSP no ha establecido ningún procedimiento que permita garantizar una homogeneidad de la información en la red de las Administraciones Públicas, no existiendo ningún recurso para determinar dónde y con qué valor de actualización se dispone en cada ente público de información personal. Cfr. L. DE SALVADOR CARRASCO, «Retos de la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos», cit., p. 206.

4. LA CANCELACIÓN DE LA INFORMACIÓN

El principio de calidad también establece que los datos de carácter personal «serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados» –art. 4.5–. No corresponde a la LAECSP establecer el plazo de conservación de los documentos administrativos en soporte electrónico sino que esto corresponde a la legislación administrativa correspondiente(88). Sin embargo, el hecho de que la Administración electrónica ofrezca enormes posibilidades para la conservación de la documentación administrativa en un soporte electrónico no justifica una conservación ilimitada de ésta cuando ya no sea necesaria –no tenga valor probatorio– o se hayan cumplido los plazos indicados en la legislación sectorial(89). Los medios electrónicos facilitan el mantenimiento íntegro de los datos «atendiendo los valores históricos, estadísticos o científicos»(90) –art. 4.5 último párrafo– así como el bloqueo de la información cuando haya dejado de ser necesaria, lo que impide el tratamiento para la finalidad inicial, conservándose únicamente los datos personales a disposición de las Administraciones Públicas y Jueces y Tribunales durante el plazo necesario para la atención de posibles responsabilidades nacidas del tratamiento –accediendo a la información únicamente aquellos empleados públicos a los que les corresponda esta puesta a disposición–. Merece una atención especial el bloqueo de la publicación de información personal en la edición electrónica de los boletines oficiales cuando se haya cumplido la finalidad que la justificó –por ejemplo, la notificación al interesado en virtud de la previsión del art. 59.5 de la LRJAP y PAC–, una cuestión que hemos abordado en otro momento(91).

---

(88) El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, señala en el art. 52 que «los períodos mínimos de conservación de los documentos electrónicos se determinarán por cada órgano administrativo de acuerdo con el procedimiento administrativo de que se trate, siendo en todo caso de aplicación, con la excepción regulada de la destrucción de documentos en papel copiados electrónicamente, las normas generales sobre conservación del patrimonio documental con valor histórico y sobre eliminación de documentos de la Administración General del Estado y sus organismos públicos». En el caso de las historias clínicas, el plazo mínimo de conservación de cinco años está establecido en la Ley 41/2002, de 14 de noviembre –art. 17.1–.

(89) La finalización de un procedimiento no supone que se tenga que borrar los datos personales del repositorio pues estos repositorios tienen como finalidad almacenar información que sirva para otros procedimientos administrativos, especialmente aquellos que pueda iniciar el ciudadano. No obstante, es necesaria la supresión de la información personal que obra en un repositorio común pasado un plazo razonable que debe determinar el responsable del fichero.

(90) Si bien los medios electrónicos favorecen más la conservación de la información que el soporte en papel, cuando esta conservación está destinada a un período de tiempo muy amplio –por ejemplo, para fines históricos o científicos–, es necesario tener en cuenta la rápida obsolescencia tecnológica de algunos sistemas que puede ocasionar un problema de compatibilidad de formatos para el acceso por los nuevos sistemas. Cfr. L. De Salvador Carrasco, «Retos de la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos», cit., pp. 212-213.

(91) El principio de calidad establece la prohibición de tratamientos excesivos, obli-

El principio de calidad anima a no conservar los datos «en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados» –art. 4.5 segundo párrafo LOPD–(92). No se trata sólo de

---

gando a la cancelación de la información cuando los datos de carácter personal hayan dejado de ser necesarios o pertinentes para la finalidad. Hay muchos supuestos donde la publicación de la información personal en Internet ha cumplido ya su finalidad por lo que se debe dejar de publicar esa información. Esto ocurre, por ejemplo, con la publicación en el diario oficial de resoluciones administrativas –por ejemplo, relativas a sanciones o a responsabilidades patrimoniales– como medio de notificación al interesado, una publicación cuya finalidad termina cuando se haya cumplido el plazo de recurso. Como hemos señalado en otro momento, la publicación de una información personal en un Boletín o diario oficial en papel no era fácilmente localizable y se restringía a una zona geográfica; en cambio la publicación en Internet de un diario o boletín oficial y su accesibilidad permanente a través de motores de búsqueda –que permiten la localización de datos personales de personas físicas que aparezcan publicados en dichos medios– da una imagen de actualidad y permanencia a una información que en muchas ocasiones ya no tiene ese carácter y que no refleja con veracidad la situación actual del afectado. Esta limitación de la publicidad de aquella información personal cuando se ha cumplido la finalidad no afecta a la autenticidad, integridad e inalterabilidad del contenido del boletín oficial –que no se modifica–; lo único que hace es limitar un tipo de tratamiento, manteniéndose su contenido a disposición de los interesados, las Administraciones Públicas y los Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento. Es especialmente adecuado en este punto la adopción de medidas técnicas necesarias –como las herramientas del tipo no robot–, que impidan la indexación automática de la información personal dentro de un boletín realizada por los motores de búsqueda generales así como por los motores de búsqueda del propio boletín. Esta fórmula permite mantener la buscabilidad del resto del diario oficial, limitando únicamente la de aquellos datos personales cuya publicación ha cumplido su finalidad. Aunque se mantuviera esta información personal en la versión electrónica del diario oficial, esta limitación de la indexación por los motores de búsqueda excluiría esta información del objeto del derecho fundamental a la protección de datos personales ya que el diario oficial en papel, aunque sea accesible a través de Internet, no está estructurado en virtud de personas. Lógicamente, la principal responsabilidad en ordenar la limitación de la buscabilidad recae en el órgano administrativo que ordenó publicar esa información administrativa en Internet y no en los motores de búsqueda –sin perjuicio de que éstos sean también responsables de su propio tratamiento–. Hay que recordar que en el Informe de 4 de abril de 2008 el Grupo de Trabajo del Artículo 29 ha afirmado que el período de conservación de datos personales por parte de dichos buscadores no debería sobrepasar los seis meses de plazo. Todas estas cuestiones las hemos analizado más ampliamente en nuestro trabajo «Transparencia administrativa y protección de datos personales», cit., pp. 67-75.

(92) La Resolución de la Agencia de Protección de Datos de la Comunidad de Madrid, de 29 de julio de 2009, declaró a la Dirección General de Movilidad del Ayuntamiento de Madrid una infracción grave prevista en el art. 44.3.d) de la LOPD por vulneración del principio de calidad en el procedimiento seguido para la atribución a los agentes de movilidad de firma electrónica en la implantación de un sistema de tramitación electrónica de denuncias de tráfico a través de las PDA. El tratamiento excesivo se produjo porque transcurrió más de un año desde que se les pidió a los agentes sus datos personales para gestionar la firma y los certificados digitales, permaneciendo su firma y certificados con su clave de seguridad almacenada todo ese tiempo en los ordenadores de la Administración hasta que se grabó el certificado con su clave de seguridad en una tarjeta criptográfica para la tramitación de multas y en un CD para que lo pudieran emplear en su

reducir el número de datos personales, evitando el tratamiento innecesario, sino de suprimir en la medida de lo posible los datos personales, facilitando la anonimización pasado el plazo necesario para el cumplimento de la finalidad. Las nuevas tecnologías permiten la anonimización automática, algo que en el soporte papel no sólo es una operación lenta y costosa sino también con un importante margen de error(93). Así, por ejemplo, las personas que utilicen comunicaciones electrónicas pueden permanecer no identificadas por los proveedores de servicios, por terceras partes que no intervienen en la transmisión del mensaje y por el receptor, a través de un sistema de encriptación(94). En este sentido, era importante la cancelación de los datos de tráfico o su anonimización, una vez cumplida la finalidad de la comunicación o la facturación de la misma(95). Así, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo prohibía el almacenamiento de los datos de tráfico relativos al establecimiento de estas comunicaciones más allá del tiempo necesario para la transmisión y la facturación, sin el consentimiento del interesado(96). Sin embargo, el interés público en la protección de los datos

caso para sus gestiones privadas. La Ley 59/2003, de 19 de diciembre, de Firma Electrónica señala la temporalidad de los datos recogidos para la creación de la firma electrónica y la inmediatez del tratamiento, prohibiendo su almacenamiento. Ya hemos señalado en otro momento cómo la modificación del art. 44.3.d) de la LOPD por el nuevo art. 44.3.c) a través de la Ley 2/2011, de 4 de marzo, circunscribe el tipo a la vulneración del principio de calidad.

(93) La Comunicación ya citada de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) –*loc. cit*–, como ya hemos señalado antes, al definir PET –tomándolo del Proyecto Pisa–, insiste en que son «un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información». Así, se establece el objetivo de «minimizar el tratamiento de datos personales y emplear datos anónimos o seudónimos cuando sea posible». La anonimización automática de los datos tras un lapso de tiempo determinado obedece al principio de que los datos tratados deben guardarse en una forma que permita identificar al interesado únicamente durante el tiempo necesario para los fines iniciales para los cuales se facilitan los datos. De esta forma, la aplicación de PET «puede ayudar a diseñar sistemas y servicios de información y comunicación que reduzcan al mínimo la recogida y el empleo de datos personales y faciliten el cumplimiento de la normativa sobre protección de datos».

(94) Uno de los principios que plantea Poullet es el de encriptación y anonimato reversible. Cfr. Y. Poullet con la colaboración de J.-D. Dinant, «Hacia nuevos principios de protección de datos en un nuevo entorno TIC», *loc. cit.*

(95) La relación de los datos de tráfico no sólo con el derecho fundamental a la protección de datos sino también con el secreto de las comunicaciones ha sido analizado por M. De los Reyes Corripio Gil-Delgado, *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet*. Agencia de Protección de Datos, 2000 y J. J. Fernández Rodríguez, *Secreto de las comunicaciones e Internet*, Civitas, Madrid, 2004.

(96) La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, estableció el deber de retención de datos de tráfico, relativos a las comunicaciones electrónicas generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, por un período máximo de doce meses –art. 12–.

personales, que animaba el anonimato de las comunicaciones electrónicas, se ha visto superado por la voluntad política materializada en normas jurídicas de limitar el derecho a la protección de datos personales para facilitar la persecución de determinados delitos –pornografía infantil– y la seguridad nacional. Por ello recientemente la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, que modifica el art. 15 de la anterior Directiva 2002/58/CE, ha permitido la conservación de los datos de tráfico por un plazo de tiempo más amplio para proteger la seguridad nacional, la defensa, la seguridad pública o la prevención, investigación, detección y enjuiciamiento de delitos, o para la utilización no autorizada del sistema de comunicaciones electrónicas. En esta dirección, se ha aprobado recientemente la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación, que establece la obligación de los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones de conservar respecto al acceso a Internet los datos de identificación del usuario asignado y el nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes generales especiales –art. 1–.

5. EL DNI ELECTRÓNICO: FINALIDAD Y DATOS OBJETO DE TRATAMIENTO

El DNI electrónico ha planteado un conjunto de implicaciones en relación con la protección de datos personales(97) y, en especial, res-

(97) El Grupo del Artículo 29, en el documento antes citado, lleva a cabo un trabajo de campo sobre la legitimidad de los identificadores únicos en los distintos países de la Unión Europea. Señala, en primer lugar, que, hasta ahora, sólo Bélgica, Dinamarca, España, Finlandia, Irlanda, Italia, Luxemburgo, Noruega y Suecia han implantado un identificador único y general a escala nacional. En otros países existen proyectos de desarrollo de identificadores únicos, en particular en Austria, pero únicamente como un número de origen oculto para los identificadores sectoriales. En Dinamarca, Bélgica y España, este identificador único convive con los sectoriales, mientras que en los otros países sólo existen identificadores sectoriales: Alemania (número de la seguridad social, número del pasaporte), Francia y Portugal (básicamente, número de la seguridad social) y Grecia y los Países Bajos (identificador relativo a los impuestos sociales, en particular). Igualmente señala que en países como Alemania y Portugal se considera inconstitucional establecer un identificador único. Hay que recordar que en este punto la Directiva 95/46/CE se limita a señalar que «[l]os Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento».

pecto al principio de calidad –la finalidad del DNI electrónico y los datos personales que pueden ser tratados–(98). La Ley Orgánica 1/1999, de 21 de febrero, de Protección de la Seguridad Ciudadana establece los principios básicos sobre tenencia y utilización del Documento Nacional de Identidad. Su finalidad es clara: acreditar la identidad de las personas. La Ley delimita los datos que necesariamente deben figurar en el DNI –la fotografía y la firma del titular– así como otros datos que se determinen reglamentariamente, prohibiendo expresamente el tratamiento de datos relativos a raza, religión, opinión, ideología, afiliación política o sindical o creencias. La creación del DNI electrónico está habilitada expresamente por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica que en su art. 15 señala que el DNI electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documento, acreditando la integridad de los documentos firmados. La LAECSP establece que los ciudadanos podrán utilizar los sistemas de firma electrónica incorporados al Documento Nacional de Identidad para identificarse y garantizar la autenticidad e integridad de los documentos electrónicos –art. 13–.

Por tanto, el tratamiento de los datos personales en el DNI-e tiene dos finalidades: acreditar la identidad y permitir la firma electrónica de documentos. El art. 11 del Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del DNI y sus certificados de firma electrónica establece los datos que debe contener el DNI-e(99). La puesta en marcha del DNI electrónico debe ser analizada cuidadosamente a la luz del principio de calidad, que exige que los datos tratados se ajusten a la finalidad y que se respete el principio de proporcionalidad y de prohibición de exceso(100). Todos los datos se tratan para acreditar la identi-

(98) Véanse las comparecencias del Director de la Agencia Española de Protección de Datos y del Presidente de la Comisión de Libertades e Informática en la Comisión de la Sociedad de la Información y del Conocimiento para dar su opinión sobre el Documento Nacional de Identidad Electrónico –*Boletín de las Cortes Generales*, VIII Legislatura. Comisiones, nº 254, año 2005–.

(99) Estos datos son: filiación, imagen digitalizada de la fotografía, imagen digitalizada de la firma manuscrita, plantilla de la impresión dactilar, certificados reconocidos de autenticidad y de firma y certificado electrónico de la autoridad emisora, que contendrán sus respectivos períodos de validez, y las claves privadas necesarias para la activación de los certificados citados. Este Real Decreto ha sufrido una modificación puntual a través del Real Decreto 1586/2009, de 16 de octubre.

(100) Así, la Comisión de Libertades Informáticas –CLI– ha criticado la puesta en marcha del DNI electrónico. Para la CLI, el DNI-e es un documento oficial que se crea con el objetivo de autenticar la identidad de su titular y no debe incluir en el chip más datos que los necesarios para la identificación. Éstos serían la plantilla con la huella dactilar, el certificado de firma, el certificado de la autoridad emisora y las claves. El resto de los datos –como los de filiación, la fotografía digitalizada y la firma manuscrita digitalizada– no deben incluirse en el chip del DNI-e, al estar produciéndose una identificación presencial. No se ofrece tampoco al ciudadano la posibilidad de oponerse a la identificación electrónica. Se cita, así, el caso de Bélgica donde la firma electrónica se activa a petición del ciudadano. En todo caso hay que recordar que en el momento de la tramitación de la Ley de Firma Electrónica, el Grupo Socialista, en-

dad y permitir la firma electrónica de documentos. Si bien existe una preocupación por el tratamiento de los datos biométricos, hay que señalar que éstos cumplen la finalidad de identificación(101). Además, estos no son datos de salud ni datos especialmente protegidos, aunque plantean la problemática de que el cuerpo humano sea detectado o sea legible por las máquinas. No obstante, una acumulación de datos adecuados puede conllevar un tratamiento desproporcionado. Por tanto, no tendría sentido una acumulación excesiva de datos biométricos en el DNI-e con una finalidad de identificación cuando ya determinados datos personales cumplen esa función(102).

El problema está en si en el futuro se incluyen en el DNI-e otros datos que se separen de las finalidades antes descritas. Cuantos más datos se incorporen al DNI-e, más riesgos existen para el principio de calidad, por un tratamiento excesivo por la propia Dirección General de la Policía o por las Administraciones Públicas, que, si no se implementan las medidas técnicas adecuadas, accederían a una información no necesaria o excesiva para la mera comprobación de la identificación. Para el Director de la Agencia Española de Protección de Datos, la incorporación de otros datos al DNI electrónico lo convertiría en un documento distinto del regulado en la Ley de Firma Electrónica, lo que exigiría una nueva habilitación legal, que estableciera las finalidades precisas y concretas, indicando cuáles serían los datos adecuados pertinentes y no excesivos para esa finalidad(103). La realidad es que existen tarjetas de identidad electrónica sectorial en Bélgica, Holanda y Finlandia y proyectos de implantación de tarjetas de esa naturaleza en Alemania, Suecia, Francia y Portugal(104). Los fines de estas tarjetas de identidad electrónica suelen ser los siguientes: firma electrónica de documentos y medios para la realización de transacciones electrónicas en todos los casos, especialmente en procedimientos administrativos en línea; tarjeta de pago en Alemania, Italia, Austria, Portugal y Suecia; tarjeta sanitaria en Alemania y Finlandia; identificador de la Seguridad Social en Alemania y Finlandia y dispositivo para el voto electrónico en Alemania, Italia y Países Bajos. A nuestro entender, no nos parece contrario al principio de calidad el tratamiento de otros datos adicionales como los relativos al permiso de conducir y el documento que visualice el saldo de puntos, que dispone una habilitación

---

tonces en la oposición, criticó que no se podía despachar el DNI-electrónico, un tema que afecta a derechos fundamentales, con tres artículos de una Ley ordinaria.

(101) Cfr. nuestra «Introducción» a *An approach to data protection in Europe*, Civitas-APDCM, Madrid, 2007, pp. 36-55.

(102) El principio de prohibición de exceso que veda el tratamiento excesivo de datos adecuados y pertinentes en el ámbito de los documentos de identificación ha sido analizado en «El principio de calidad de los datos», cit., pp. 346-346.

(103) Véase la comparecencia del Director de la Agencia Española de Protección de Datos antes citada.

(104) Esta cuestión ha sido también abordada por el Grupo de Trabajo del art. 29, en el documento de trabajo sobre administración electrónica, de 8 de mayo de 2003, citado anteriormente.

expresa en la Ley 17/2005, de 19 de julio, que regula el permiso y la licencia de conducción por puntos(105). La seguridad vial no es una finalidad sólo administrativa sino también policial y el carné de conducir cumple una finalidad de identificación semejante al DNI. No parece razonable la inclusión de otros datos como los relativos a la salud, ya que tienen una finalidad distinta a la policial y el acceso de las Fuerzas y Cuerpos de Seguridad del Estado a los datos de salud se encuentra limitado a los supuestos donde exista un peligro real para la seguridad pública o cuando sea necesario para la persecución de delitos o de delincuentes(106).

IV. LA INFORMACIÓN Y EL CONSENTIMIENTO PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA

1. LA INFORMACIÓN AL INTERESADO DE LOS DISTINTOS TRATAMIENTOS (ACCESOS, CESIONES INDIVIDUALIZADAS, INTERCONEXIONES, COMPROBACIONES AUTOMATIZADAS, VERIFICACIÓN DE LA AUTENTICIDAD DE LA INFORMACIÓN)

La Administración electrónica debe tener en cuenta especialmente el principio de información en la recogida de datos –art. 5 LOPD–. El ciudadano que utilice medios electrónicos para relacionarse con la Administración Pública tiene que estar informado previamente de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento con sus datos personales, de la finalidad de éste, de los destinatarios de la información y de la identidad y dirección del responsable del fi-

(105) En todo caso, un documento administrativo que incorpore datos adicionales dejaría de ser un DNI electrónico, aunque podría ser legítimo si se encuadra en la existencia de funciones administrativas legítimas y no requerirían necesariamente una habilitación legal. No obstante, como hemos señalado anteriormente muchos países prohíben en sus legislaciones la existencia de un número único de identificación de los ciudadanos.

(106) La separación de las distintas finalidades –y los datos necesarios para su cumplimento– en distintos soportes es lo más adecuado desde la perspectiva de la seguridad porque garantiza la confidencialidad de la información y evita accesos a datos por personas no autorizadas y que no tienen la competencia administrativa. Obviamente, la tecnología permite el almacenamiento de información en el mismo documento para finalidades distintas estableciendo medidas de seguridad que separen técnicamente los niveles de acceso. Cfr. J. VALERO TORRIJOS y D. SÁNCHEZ MARTÍNEZ, «Protección de datos personales, DNI-e y prestación de servicios de certificación: ¿un obstáculo para la e-Administración?», *Datospersonales.org. Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº 25, 2007. Así, por ejemplo, la inclusión de datos de salud en documentos de identificación puede conllevar la inclusión de información de naturaleza religiosa que pueda ser utilizada en caso de urgencia. Cfr. L. MARTÍN-RETORTILLO BAQUER, «¿Hacer constar la religión en el carné de identidad? (Tribunal Europeo de Derechos Humanos: Decisión sobre admisibilidad "Sofianopoulos, Spaïotis, Metallinos y Kontogiannis c. Grecia", de 12 de diciembre de 2002», *Revista Española de Derecho Administrativo*, nº 128, 2005, pp. 683 a 694.

chero(107). También será necesario informar al titular de los datos del carácter obligatorio o facultativo de la respuesta, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos y de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición cuando esta información no pueda deducirse claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban –art. 5.3 LOPD–(108). El cumplimiento del principio de información es esencial para permitir el control sobre los propios datos personales en un ámbito como el de las Administraciones Públicas donde no está presente frecuentemente el consentimiento del interesado. Es especialmente importante garantizar el principio de información al interesado cuando los servicios de Administración electrónica vayan a proceder al tratamiento de datos especialmente protegidos. Además, el principio de información permite mejorar la confianza del ciudadano en la Administración en línea, siendo además un buen instrumento para concienciar a éste sobre su derecho fundamental a la protección de datos personales(109).

El derecho a la información debe materializarse en el mismo soporte donde se recogen los datos personales. Así, la normativa administrativa que aprueba los formularios electrónicos oficiales para la recogida de datos debe incluir en éstos una leyenda donde se indique «en forma claramente legible» –art. 5.2 LOPD– la existencia de un tratamiento de datos personales, su finalidad, la comunicación de los datos a otros órganos, quién es el responsable y los derechos del interesado. Si bien las solicitudes impresas donde se recaban los datos personales en papel disponen también de leyendas informativas, la tramitación electrónica ofrece una oportunidad a los poderes públicos para informar, impidiendo al mismo tiempo el envío de la solicitud si no se ha leído la cláusula informativa(110). Esta información debe ofrecerse al interesado cuando

(107) Para un análisis del principio de información en la recogida de datos, cfr. A. Troncoso Reigada, «Introducción» a *Principios y derechos de protección de datos personales. Doctrina de la Agencia de Protección de Datos de la Comunidad de Madrid 2002-2009*, Civitas-APDCM, 2010, pp. 144-150.

(108) Así, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, establece como contenido mínimo de las sedes electrónicas la identificación de la sede, así como del órgano u órganos titulares y de los responsables de la gestión; las normas de creación del registro o registros electrónicos accesibles desde la sede; y la información relacionada con la protección de datos de carácter personal, incluyendo un enlace con la sede electrónica de la Agencia Española de Protección de Datos –art. 6.1.g)–.

(109) Cfr. más ampliamente el Documento del Grupo de Trabajo del Artículo 29, «Recomendación sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea», 17 de mayo de 2001, ya citado.

(110) Así, por ejemplo, para incorporar información personal se puede establecer como requisito previo el acceso a una ventana que contenga una cláusula informativa especifica en relación con los datos personales recabados para el servicio de Administración electrónica que se pretenda usar, exigiendo una actuación activa por parte del ciudadano, por ejemplo, obligándole a marcar una determinada casilla indicando que se ha accedido a la ventana de informa-

visita la oficina virtual, de manera que no pueda presentar un escrito sin que la Administración haya cumplido su deber de información. Sin embargo, son todavía muchos los formularios *on line* de las Administraciones Públicas que no incluyen la leyenda informativa o no cumplen con exactitud el principio de información en la recogida de datos(111). La Administración no sólo lleva a cabo un tratamiento de datos personales a través de documentos electrónicos normalizados dentro de procedimientos administrativos sino que también recibe a través de registros electrónicos, direcciones institucionales de correo electrónico o buzones electrónicos distintos escritos –quejas, sugerencias, solicitudes, etc.– donde se incluyen datos personales y donde también es necesario cumplir el principio de información. Igualmente, es preciso informar a los ciudadanos en los términos previstos en el art. 5.1 de la LOPD en la recogida de datos personales para la gestión de altas en los servicios de novedades o de alertas SMS o cuando se recaban datos personales –por ejemplo, la dirección de correo electrónico– para la participación en foros de discusión, debiéndose indicar siempre la finalidad explícita del fichero donde serán registrados los datos(112). En general hay que prestar una especial importancia a la política de privacidad en los sitios web de las Administraciones Públicas. De hecho, en muchas ocasiones cuando la recogida de datos personales se hace a través de un sitio web de la Administración, el principio de información se cumple mediante cláusulas a las que se accede a través de enlaces como pueden ser «aviso legal» o «política de privacidad». Es importante que esta política de privacidad sea accesible y que el ciudadano comprenda que le están informando de sus derechos(113).

Merece una mención específica la utilización de *cookies* en los servicios de Administración electrónica, un sistema de seguimiento de la nave-

---

ción y bloqueando el acceso al servicio en el caso de que no se haya marcado y visualizado la ventana correspondiente. Cfr. la Recomendación 3/2008, de 30 de abril, de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica.

(111) Esto es especialmente evidente cuando la Administración recaba datos personales fuera de los formularios electrónicos. Esta es una cuestión que la Agencia de Protección de Datos de la Comunidad de Madrid analizó en el Plan de Inspección sobre los servicios de Administración electrónica y la política de privacidad en las Corporaciones Locales de la Comunidad de Madrid que se impulsó durante el año 2008 –ya mencionado anteriormente–.

(112) Cuando el tratamiento de datos personales sea de menores de edad –por ejemplo, para suscribirse a un foro–, la información dirigida a éstos debe estar en un lenguaje fácilmente comprensible –art. 13.3 del Reglamento de desarrollo de la LOPD–.

(113) Así, en la página de inicio de los sitios web debería aparecer en lugar destacado la «Política de privacidad», donde se ofreciera una información fácilmente comprensible de la titularidad del sitio web, de la finalidad del mismo, de las medidas técnicas de seguridad adoptadas –por ejemplo, para evitar determinadas búsquedas basadas en datos de carácter personal o la utilización de herramientas que permitan el tratamiento de los datos de tráfico por parte de terceros–, de la protección de datos de carácter personal, del posible uso de *cookies* y otros tratamientos invisibles y del posible uso de la dirección IP del usuario. También la política de privacidad puede informar al interesado que en la web no se recogen datos de carácter personal. Cfr. en este sentido la Recomendación 3/2008, de 30 de abril, ya citada.

gación en Internet que supone un tratamiento de datos personales y que requiere siempre con carácter previo la información al interesado sobre la existencia del mismo –que la mayoría de las veces desconoce–, su finalidad, los destinatarios de la información, la identidad del responsable y los derechos que le asisten. La Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas señala –art. 5.3– que «[l]os Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado».

El derecho de información en la recogida de los datos exige una información expresa, precisa e inequívoca también en relación con los destinatarios o cesionarios de la misma –art. 5.1.a) LOPD–. Es especialmente importante la información al ciudadano sobre las cesiones de datos entre Administraciones Públicas –accesos electrónicos, interconexiones, comprobaciones de copias digitales de los documentos, verificaciones de la autenticidad de los datos contenidos en las solicitudes, etc.–, especialmente cuando estas cesiones se realizan sin su consentimiento en virtud de una habilitación legal ya que sólo conociendo quién tiene sus datos personales puede el ciudadano controlar de alguna manera el uso de su información personal(114). Además, cuando un ciudadano en un procedimiento donde es necesario aportar certificaciones y documentos de otras Administraciones Públicas se acoge al derecho «a no aportar los datos y documentos que estén en poder de las Administraciones Públicas las cuales utilizarán medios electrónicos para recabar di-

(114) Para el Grupo del Artículo 29, «[s]in tal información, el consentimiento personal sería ilusorio, pues no habría ninguna razón justificada para rechazar la comunicación de los datos frente al argumento de la simplificación de los procedimientos administrativos». Así, «[d]icha información ha de ser lo suficientemente precisa como para que las personas puedan entender realmente los riesgos potenciales que conlleva la transmisión de sus datos y las consecuencias que ésta podría inducir». En particular, el documento de trabajo de este Grupo recomendó que los proveedores de servicios de certificación «facilitarán al usuario información clara acerca de la comunicación de los datos, en cumplimiento de las normas de comunicación de datos personales». –Documento de trabajo sobre la Administración en línea, cit.–.

cha información» –art. 6.2.b) LOPD–, es necesario informarle previamente de manera expresa, precisa e inequívoca, de que van a producirse accesos y cesiones de datos entre Administraciones Públicas. En esta dirección, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, procura dar cumplimientos a las exigencias de una información, previa, expresa, precisa e inequívoca, señalando que los interesados serán informados expresamente de que el ejercicio del derecho implica su consentimiento, en los términos establecidos por el 6.2.b) de la LAECSP, para que el órgano y organismo ante el que se ejercita pueda recabar los datos o documentos de otras Administraciones Públicas y de que el derecho del art. 6.2.b) de la LAECSP se ejercita de forma específica e individualizada para cada procedimiento concreto, sin que implique un consentimiento general referido a todos los procedimientos que una Administración tramite en relación con el interesado –art. 2–. El Real Decreto 1671/2009, de 6 de noviembre, establece que los órganos ante los que se ejercite el derecho del art. 6.2.b) de la LAECSP conservarán la documentación acreditativa del efectivo ejercicio del derecho incorporándola al expediente en que el mismo se ejerció, lo que prueba, como señalaremos más adelante, la existencia de un consentimiento para la cesión. Igualmente, es necesario informar al interesado de la posible cesión de datos entre Administraciones Públicas que se produce si éste aporta a un expediente copias digitalizadas de documentos ya que la Administración puede solicitar del correspondiente archivo la comprobación de las copias aportadas –art. 35 LAECSP–. También es necesario garantizar el principio de información del art. 5 de la LOPD cuando la inclusión en una solicitud dirigida a la Administración de datos personales implica la posibilidad de que la Administración destinataria de la solicitud verifique esta información en otras bases de datos públicas para comprobar la autenticidad de la información –una previsión que requiere el consentimiento tácito después de cumplir el principio de información–(115). Como señalaremos más adelante, es muy importante que el responsable del fichero garantice que ha cumplido el principio de información previa, expresa, precisa e inequívoca porque sólo así es posible afirmar que existe, en su caso, un consentimiento informado y un consentimiento manifestado de manera tácita. Igualmente, cuando los datos recabados en un servicio de Administración electrónica, o los generados en cualquier acto de trámite o en la resolución del correspondiente procedimiento administrativo vayan a ser incorporados a repositorios de datos o documentales, con el fin de facilitar el derecho a no aportar datos que ya obren en poder de la Administración se deberá informar expresamente de tal hecho al ciudadano(116).

---

(115) Como más adelante analizaremos, la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de julio de 2010 –Sección Sexta– ha anulado el art. 11 del Reglamento de desarrollo de la LOPD relativo a las «Verificaciones de datos en solicitudes formuladas a las Administraciones Públicas».

(116) Cfr. la Recomendación 3/2008 de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica.

La LOPD obliga al responsable del fichero a informar al interesado dentro de los tres meses siguientes al registro de los datos del contenido del tratamiento, de la procedencia de los datos, de la finalidad, de la identidad y dirección del responsable y de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición –art. 5.4–, salvo que ya hubiera sido informado con anterioridad, una disposición legal así lo prevea, el tratamiento de los datos tenga una finalidad histórica, estadística o científica o la información al interesado resulte imposible o exija esfuerzos desproporcionados a juicio de la autoridad de control en consideración al número de interesados o a la antigüedad de los datos –art. 5.5 LOPD–(117).

No obstante, las nuevas tecnologías, como hemos señalado anteriormente, son también una oportunidad para el mejor cumplimiento del principio de información. Además, los medios electrónicos facilitan al responsable la prueba o la acreditación del cumplimiento de este deber de información. Como es sabido, el art. 18 del Reglamento de desarrollo de la LOPD, que llevaba por título «Acreditación del cumplimiento del deber de información», exigía que el deber de información se realizara por cualquier medio que permitiera acreditar su cumplimiento y obligaba a conservar el medio o soporte a través del cual se había cumplido este deber(118). La Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo –Sección Sexta–, de 15 de julio de 2010, ha anulado este precepto del Reglamento, entendiendo que no sólo obligaba a cumplir el deber de información sino exigía que la prueba del cumplimiento del deber de información constara documentalmente o por medios informáticos, lo que representaba una obligación adicional al responsable del fichero no prevista en la Ley, que dejaba libertad de forma a la hora de informar al interesado y de probar el cumplimiento del deber de información(119). Hay que dejar claro que el responsable del fichero y trata-

(117) Cfr. E. GUICHOT REINA, *Datos personales y Administración Pública*, cit., pp. 390 a 391.

(118) El art. 18 del Reglamento de desarrollo de la LOPD decía: «1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado. 2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.»

(119) La Sentencia señala –en el Fundamento Jurídico Noveno– que «no se limita dicho precepto [el art. 18 del Reglamento] a poner de manifiesto que la carga de probar el efectivo cumplimiento del deber de informar corre a cargo del responsable del fichero o tratamiento. Lo que en realidad establece es la obligación de que la prueba de ese efectivo cumplimiento conste documentalmente o por medios informáticos o telemáticos. Y aunque no es posible inferir, como con error sostiene la recurrente, que la norma reduce el derecho a probar por cualquier medio de los admitidos en derecho, sí tiene razón cuando aduce que establece *ex novo*, al margen de la Ley, una obligación adicional. Es más,

miento sigue teniendo la obligación de informar de manera previa, expresa, precisa e inequívoca de lo previsto en el art. 5 de la LOPD y de acreditar el cumplimiento del deber de información, ya que sobre él recae la carga de la prueba. El consentimiento, que además está referido a un tratamiento o tratamientos concretos, es un consentimiento *informado* –art. 3.h) LOPD– y el responsable también está obligado a probar la existencia de este consentimiento *informado* «por cualquier medio de prueba admisible en derecho» –art. 12.3 del Reglamento de desarrollo de la LOPD–(120), por lo que se mantiene una doble obligación de probar el cumplimiento del principio de información, para lo cual debe disponer de un medio de prueba admisible en Derecho que lo demuestre. Por eso, es aconsejable tener en cuenta –no como obligación pero sí como Recomendación, como señala la propia Sentencia del Tribunal Supremo– la previsión anulada que preveía que el responsable acuda a medios informáticos o telemáticos para conservar el soporte en el que coste el cumplimiento del deber de informar, y, en particular, proceda al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales. La existencia de medios electrónicos también impide en muchas ocasiones que el responsable se pueda acoger a la exoneración del deber de información cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados –art. 5.5 LOPD–. Por último, la Comunicación que recientemente ha enviado la Comisión al Parlamento Europeo y al Consejo relativa al fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET)

---

con la obligación impuesta en el precepto reglamentario puede originar que se aprecie con un cierto grado de desconfianza la conducta de quienes pudiendo preconstituir, sin grandes dificultades apreciables, un medio probatorio exigido por el Reglamento, hace caso omiso a la exigencia. La Ley reconoce en el artículo 5 el derecho a la información en la recogida de datos, concreta el contenido de la información, y advierte de que el deber de informar ha de ser previo a la recogida, pero salvo la indicación de que la información ha de ser expresa, precisa e inequívoca, ninguna referencia contiene a la forma, abriendo así múltiples posibilidades (escrita, verbal, telemática, etc.). Solo en el apartado 2 del artículo de mención prevé la posibilidad de que se utilicen cuestionarios u otros impresos para la recogida de datos para advertir, pensando sin duda en medios estandarizados, que se han de contener y de forma claramente legible las advertencias expresadas en el apartado 1. En consecuencia, debe considerarse que el legislador ha optado por la libertad de forma. Pues bien, siendo ello así, cabe concluir que la disposición reglamentaria que examinamos contraviene la Ley y que por ello debe ser anulada. Solución distinta se alcanzaría si la letra del precepto impugnado pudiera interpretarse en el sentido de que el medio que previene para cumplir el deber de información se realiza como una mera recomendación, «ad cautelam» de una dificultad probatoria futura, pero los términos categóricos e imperativos utilizados *("deberá llevarse a cabo", "deberá conservar el soporte")*, impiden esa valoración. En consecuencia, la impugnación del artículo 18 del Reglamento debe estimarse».

(120) Llama la atención que el Reglamento de desarrollo de la LOPD permitiera acreditar el consentimiento del interesado «por cualquier medio de prueba admisible en derecho», siendo menos flexible en el art. 18 a la hora de establecer la forma de acreditar el cumplimiento del deber de información.

–que trata de potenciar que las TIC sean un instrumento que proteja este derecho, sin perjuicio de su funcionalidad–, menciona la Plataforma de Preferencias de Privacidad (P3P), «que permite a los usuarios de Internet analizar la política de los sitios web por lo que se refiere a la intimidad y compararla con las preferencias del usuario en relación con la información que desee facilitar, y contribuye a garantizar que el interesado autoriza el tratamiento de sus datos con conocimiento de causa»(121).

2. EL CONSENTIMIENTO DEL INTERESADO PARA EL TRATAMIENTO DE SUS DATOS EN LOS SERVICIOS DE ADMINISTRACIÓN ELECTRÓNICA PARA EL CUMPLIMIENTO DE FUNCIONES ADMINISTRATIVAS Y PARA ACTIVIDADES COMPLEMENTARIAS (SERVICIOS DE NOTICIAS Y ALERTAS Y USO DE «COOKIES»)

La utilización de las nuevas tecnologías permite materializar el consentimiento del interesado para el tratamiento de sus datos –art. 6.1 LOPD–. Esto es especialmente importante en los servicios electrónicos que son responsabilidad de personas jurídico-privadas ya que pueden obtener más fácilmente la prueba del otorgamiento del consentimiento. En el caso de la Administración electrónica en muchas ocasiones no es necesario recabar el consentimiento del interesado para el tratamiento de sus datos personales porque existe una habilitación legal, los datos se recogen para ejercicio de funciones administrativas o se refieren a las partes de una relación laboral o administrativa siendo la información necesaria para su mantenimiento y cumplimiento–art. 6.2 LOPD–(122), lo que no exime del cumplimiento de otros principios de protección de datos como el de calidad o el de información(123). Una cuestión que ha suscitado controversia es si los empleados públicos tienen que dar su

(121) COM (2007) 228 final, de 2.5.2007 –*loc. cit.*–.

(122) Así, por ejemplo, las sedes electrónicas y los registros electrónicos que permiten el acceso a servicios de Administración electrónica a instancia del interesado no necesitan recabar el consentimiento del mismo para el tratamiento de sus datos. Lo mismo ocurre con los tratamientos de datos de funcionarios y empleados públicos que se desarrolla en los portales electrónicos del empleado. No obstante, como hemos señalado en otro momento, aunque muchos de los tratamientos de datos personales que llevan a cabo las Administraciones Públicas están exceptuados del consentimiento del interesado, cuando se desarrollan servicios públicos en virtud de la voluntariedad del interesado y no se prestan funciones públicas de soberanía –por ejemplo, cuando se solicita el ingreso en un centro residencial–, es más respetuoso con los derechos de las personas solicitar este consentimiento, también por medios electrónicos. A. TRONCOSO REIGADA, «Introducción» a *Principios y derechos de protección de datos personales. Doctrina de la Agencia de Protección de Datos de la Comunidad de Madrid 2002-2009*, cit., pp. 150-154.

(123) Los campos que deben ser completados de manera obligatoria en los formularios electrónicos antes de enviar la solicitud a la Administración tienen que ser analizados a la luz del principio de adecuación y prohibición de exceso. Especialmente hay que valorar no sólo la pertinencia de un dato personal para la finalidad sino el hecho de que sea un campo obligatorio para poder enviar la solicitud ya que esto supone un límite a la posibilidad de subsanación establecida en el art. 70 de la LRJ-PAC.

consentimiento para el tratamiento de sus datos personales cuando se les entrega el certificado electrónico, teniendo en cuenta que en ellos aparece visible su número de DNI. La Ley 59/2003, de 19 de diciembre, de Firma Electrónica se fundamenta claramente en el consentimiento del interesado al establecer que para la expedición de certificados electrónicos al público los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos y los datos no podrán ser tratados con fines distintos sin el consentimiento expreso del firmante –art. 17–. Sin embargo, el cumplimiento de funciones propias de las Administraciones Públicas en el ámbito de sus competencias así como la existencia de una relación administrativa –en este caso, de sujeción especial– entre un empleado público y su Administración permiten, como hemos señalado antes, que ésta lleve a cabo tratamientos de datos personales sin consentimiento de éstos. Así, la atribución de un certificado electrónico a los empleados públicos para la tramitación electrónica de los documentos administrativos permite implementar el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos. Por ello, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, establece –art. 19 «Firma electrónica del personal al servicio de las Administraciones Públicas»– que «la identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad actuante, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio. Cada Administración Pública podrá proveer a su personal de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios. La firma electrónica basada en el Documento Nacional de Identidad podrá utilizarse a los efectos de este artículo». De esta forma, el tratamiento del dato del DNI para dar la firma electrónica a los empleados públicos sin consentimiento de éstos dispone también de una clara habilitación legal(124). En todo caso, la inexistencia de consentimiento del interesado no suprime el hecho de que exista un tratamiento de datos de personas físicas y que, por tanto, los empleados públicos sean titulares

(124) El Real Decreto 1553/2005, de 23 diciembre, establece que el DNI tiene como finalidad la identificación electrónica de su titular y la firma electrónica de documentos. Hay que recordar que el art. 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, establece que el documento electrónico será soporte de: a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso. b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica. La Ley 59/2003, de 19 de diciembre, de Firma Electrónica establece en el art. 11 que los certificados reconocidos incluirán la identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de Documento Nacional de Identidad o a través de un seudónimo que conste como tal de manera inequívoca.

también en este caso del derecho fundamental a la protección de datos, lo que obliga a respetar los principios y derechos de protección de datos –información, calidad, finalidad, seguridad, etc.–(125).

(125) No estamos en el supuesto contemplado en el art. 2.2 del Reglamento de desarrollo de la LOPD que señala que no será aplicable «a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que prestan sus servicios en aquéllas, consistentes únicamente en su nombre y apellido, las funciones y puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales». Si bien los empleados públicos entrarían en la categoría de personas físicas que prestan servicios en personas jurídicas, la inclusión en el certificado electrónico de los empleados públicos del dato relativo a su DNI hace que estos ficheros estén plenamente sometidos a la LOPD y a su Reglamento. Además, la finalidad del tratamiento no es entrar en contacto con las personas jurídicas en las que el empleado presta sus servicios –los llamados «ficheros de contactos»–. La Agencia Española ha considerado que los datos de las personas físicas de contacto que representan a una persona jurídica son datos de personas jurídicas, siendo el dato de la persona física meramente accidental en relación con el contenido y finalidad del tratamiento. Ya hemos criticado en otro momento las exclusiones al ámbito objetivo de aplicación del Reglamento –cfr. nuestra «Introducción» a Protección de datos personales para Administraciones Locales, Civitas–, APDCM, Madrid, 2008, pp. 18-27. A nuestro juicio, el hecho de que no sea necesario el consentimiento del interesado para algunos tratamientos no suprime la existencia de un derecho fundamental que cubre los datos de personas físicas sometidos a tratamiento –no otra cosa son los ficheros de contactos–, aunque este derecho esté sometido a límites. No obstante, la Agencia Española de Protección de Datos ha interpretado este precepto en el sentido siguiente: «En los supuestos en que el tratamiento del dato de la persona de contacto es meramente accidental en relación con la finalidad del tratamiento, referida realmente a las personas jurídicas en las que el sujeto presta sus servicios, no resulta de aplicación lo dispuesto en la Ley Orgánica 15/1999, viniendo el Reglamento a plasmar este principio. No obstante, nuevamente, es necesario que el tratamiento del dato de la persona de contacto sea accesorio en relación con la finalidad perseguida. Ello se materializará mediante el cumplimiento de dos requisitos: El primero, que aparece expresamente recogido en el Reglamento será el de que los datos tratados se limiten efectivamente a los meramente necesarios para identificar al sujeto en la persona jurídica a la que presta sus servicios. Por este motivo, el Reglamento impone que el tratamiento se limite a los datos de nombre y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales. De este modo, cualquier tratamiento que contenga datos adicionales a los citados se encontrará plenamente sometido a la Ley Orgánica 15/1999, por exceder de lo meramente imprescindible para identificar al sujeto en cuanto contacto de quien realiza el tratamiento con otra empresa o persona jurídica. Por ello, no se encontrarían excluidos de la Ley los ficheros en los que, por ejemplo, se incluyera el dato del Documento Nacional de Identidad del sujeto, al no ser el mismo necesario para el mantenimiento del contacto empresarial. Igualmente, y por razones obvias, nunca podrá considerarse que se encuentran excluidos de la Ley Orgánica los ficheros del empresario respecto de su propio personal, en que la finalidad no será el mero contacto, sino el ejercicio de las potestades de organización y dirección que a aquél atribuyen las leyes. El segundo de los límites se encuentra, como en el supuesto contemplado en el artículo 2.3, en la finalidad que justifica el tratamiento. Como se ha venido indicando reiteradamente, la inclusión de los datos de la persona de contacto debe ser meramente accidental o incidental respecto de la verdadera finalidad perseguida por el tratamiento, que ha de residenciarse no en el sujeto, sino en la entidad en la que el mismo desarrolla su actividad o a la que aquél representa en sus relaciones con quienes tratan los datos. De este modo, la finalidad del tratamiento

Además, una cosa es que no haga falta el consentimiento para el tratamiento de datos personales en el ámbito de las Administraciones Públicas –por lo que la Administración puede utilizar internamente en su *back office* medios electrónicos para la tramitación del procedimiento, pudiendo obligar a utilizar el certificado electrónico a sus cargos públicos y empleados–, y otra cosa distinta es que la Administración pueda imponer a los ciudadanos que se relacionen con ella a través de medios electrónicos. Como antes hemos analizado, la LAECSP insiste en la importancia del consentimiento del interesado para que la Administración pueda comunicarse por medios electrónicos. Así, las Administraciones Públicas utilizarán medios electrónicos en sus comunicaciones con los ciudadanos «siempre que lo hayan solicitado expresamente o consentido expresamente. La solicitud y el consentimiento podrán, en todo caso, emitirse por medios electrónicos» –art. 27.2–(126). Cuando la tramitación se inicia de oficio por la propia Administración Pública, los interesados deben de otorgar expresamente su consentimiento para la tramitación por medios electrónicos, o bien realizar actos de los que se desprenda esta aceptación. Esto es especialmente importante en la tramitación de los procedimientos sancionadores, tanto en la fase de actuaciones previas como en la de instrucción(127). El ciudadano puede elegir, en todo momento, la

---

debe perseguir una relación directa entre quienes traten el dato y la entidad y no entre aquéllos y quien ostente una determinada posición en la empresa. De este modo, el uso del dato debería dirigirse a la persona jurídica, siendo el dato del sujeto únicamente el medio para lograr esa finalidad. Así sucedería en caso de que el tratamiento responda a relaciones «business to business», de modo que las comunicaciones dirigidas a la empresa, simplemente, incorporen el nombre de la persona como medio de representar gráficamente el destinatario de la misma. Por el contrario, si la relación fuera «business to consumer», siendo relevante el sujeto cuyo dato ha sido tratado no sólo en cuanto a la posición ocupada sino como destinatario real de la comunicación, el tratamiento se encontraría plenamente sometido a la Ley Orgánica 15/1999, no siendo de aplicación lo dispuesto en el artículo 2.2 del Reglamento» –este Informe de la Asesoría Jurídica de la AEPD se encuentra accesible en su web–.

(126) Por tanto, la LAECSP exige solicitud expresa del ciudadano o consentimiento expreso del ciudadano para que la Administración pueda utilizar medios electrónicos en sus comunicaciones con éstos –un consentimiento que puede recabarse por medios electrónicos–, aunque no necesariamente a través de un sistema de identificación fuerte como la firma digital. Parece que el hecho de que un ciudadano se haya comunicado con la Administración por medios electrónicos aportando un número de identificación justifica que ésta le pueda responder por los mismos medios –otra cosa distinta es la notificación de un acto administrativo–. No obstante, se prevé también la posibilidad de que las Administraciones Públicas puedan imponer a través de un reglamento la obligatoriedad de comunicarse con ellas por medios electrónicos «cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y la disponibilidad de los medios tecnológicos precisos» –art. 27.6–.

(127) Salvador Carrasco incide en la importancia a la hora de tramitar los procedimientos sancionadores de determinar con claridad si se otorgó por el ciudadano ese consentimiento o si se denegó por el ciudadano de manera explícita sin que quede margen para la incertidumbre: «Un procedimiento para recabar el consentimiento y un registro por sí mismo no es suficiente; es necesario que dicho procedimiento garantice el no repudio del ciuda-

forma de comunicarse con las Administraciones Públicas –sea o no por medios electrónicos –art. 27.1–. Aunque el procedimiento se haya iniciado por medios electrónicos, el ciudadano –e incluso terceros interesados– pueden optar por una tramitación no electrónica por lo que la iniciación electrónica de un procedimiento administrativo no implica que todo el procedimiento se haga de manera electrónica. Igualmente, para que las notificaciones se practiquen por medios electrónicos, es necesario que el interesado haya señalado este medio como preferente o haya consentido su utilización. Tanto esta indicación de preferencia en el uso del medio electrónico como el consentimiento pueden emitirse y recabarse por medios electrónicos –art. 28.1 LAECSP–(128). Durante la tramitación del procedimiento el interesado puede requerir al órgano administrativo que las notificaciones sucesivas no se practiquen por medios electrónicos –art. 28.4–. Es especialmente importante la introducción de sistemas que permitan en el otorgamiento del consentimiento por medios electrónicos garantizar la identidad, la autenticidad y la integridad de la información, de forma que este consentimiento tenga efectos jurídicos. Así, hay operaciones que exigen una clara identificación y autenticación del ciudadano(129). La iniciación de un procedimiento administrativo de forma electrónica a instancia de parte requiere una identificación fuerte, que se realiza mediante la firma electrónica incorporada al DNI-e, mediante la firma electrónica avanzada u otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo –art. 13 LAECSP–, lo que permite otorgar plena eficacia jurídica a los documentos firmados electrónicamente(130). Esto también es aplicable al acceso

---

dano cuando otorga el consentimiento y el no repudio de la Administración Pública cuando ese consentimiento se deniega». Cfr. L. DE SALVADOR CARRASCO, «Retos de la Ley de Acceso Electrónico», cit., pp. 215-216.

(128) El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, señala igualmente en relación con el medio de notificación –art. 36– que «las notificaciones se efectuarán por medios electrónicos cuando así haya sido solicitado o consentido *expresamente* por el interesado o cuando haya sido establecida como obligatoria conforme a lo dispuesto en los arts. 27.6 y 28.1 de la LAECSP. La solicitud deberá manifestar la voluntad de recibir las notificaciones por alguna de las formas electrónicas reconocidas, e indicar un medio de notificación electrónica válido conforme a lo establecido en el presente Real Decreto. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento podrán emitirse y recabarse, en todo caso, por medios electrónicos. Cuando la notificación deba admitirse obligatoriamente por medios electrónicos, el interesado podrá elegir entre las distintas formas disponibles salvo que la normativa que establece la notificación electrónica obligatoria señale una forma específica».

(129) La LAECSP también prevé que cuando para la realización de una operación por medios electrónicos se exija la identificación o autenticación del ciudadano mediante algún instrumento de los que éste no disponga, es posible la identificación y autenticación de los ciudadanos por funcionario público mediante el uso del sistema de firma electrónica de éstos, debiendo el ciudadano identificarse y «prestar su consentimiento *expreso*, debiendo quedar constancia de ello» –art. 22–.

(130) El Grupo de Trabajo del artículo 29 siempre ha propiciado el empleo de la firma electrónica. En el ámbito financiero, el requisito de la identidad y de la autenticidad es esencial a la hora de asegurarse que la declaración de voluntad pertenece a su emisor y no es suplantada por ninguna otra

a un expediente administrativo o cuando se procede a firmar durante el procedimiento electrónico los documentos contenidos en las pruebas documentales(131).

La Administración Pública también requiere obtener el consentimiento del interesado para ofrecer determinados servicios electrónicos que no suponen el ejercicio de funciones propias de las Administraciones Públicas en el ámbito de sus competencias. Este consentimiento no tiene que ser expresado a través de un medio de identificación fuerte sino que basta con que sea una manifestación de voluntad libre, inequívoca, específica e informada –art. 3.h) LOPD–. La LOPD no requiere necesariamente que el consentimiento sea consecuencia de una afirmación expresa del afectado sino que puede ser tácito(132), siendo suficiente que no exista una manifestación en contrario al tratamiento después de una advertencia expresa(133). Lógicamente, este consentimiento tácito, ade-

---

persona. Algunas implicaciones interesantes de la firma electrónica en la protección de datos de carácter personal, especialmente en relación con la cesión de datos personales que puede suponer algunos sistemas de consulta de la información relativa a la revocación de los certificados ha sido analizado por J. VALERO TORRIJOS, «Implicaciones de la protección de datos de carácter personal para la Administración electrónica», cit., pp. 192-194.

(131) El art. 13 de LAECSP –titulado «Formas de identificación y autenticación»– contiene los distintos mecanismos para identificar al ciudadano y recabar su consentimiento. SALVADOR CARRASCO señala que la firma electrónica es una garantía de identificación y de no repudio siempre que no se comprometa la confidencialidad de la clave. Este autor apuesta por el DNI electrónico, siempre que se obligue a introducir el pin en cada una de las transacciones, y critica otros medios de identificación menos robustos como aquellos que identifican al usuario con la terminal y que pueden plantear problemas en las garantías de las notificaciones: «si la STC 128/2008, de 27 de octubre critica la simple publicación en un edicto de una sanción sin realizar una mínima actividad indagatoria para determinar el domicilio del infractor, «cómo va a aceptar la notificación a un terminal sin la garantía de quién es el usuario final del mismo». Cfr. L. SALVADOR CARRASCO, «Retos de la Ley de Acceso Electrónico», cit., pp. 215-217.

(132) La Ley 2/2011, de 4 de marzo, de Economía Sostenible ha introducido a través de su Disposición final quincuagésima sexta algunas modificaciones en la LOPD, especialmente en lo relativo al tipo de infracciones. Así, si antes era infracción grave proceder a la recogida de datos de carácter personal sin recabar *el consentimiento expreso* de las personas afectadas, en los casos en que éste sea exigible –antiguo art. 44.3.c) LOPD–, ahora se considera infracción grave tratar los datos de carácter personal sin recabar *el consentimiento de las personas* afectadas, sin exigir que este consentimiento sea expreso, pudiendo ser tácito –nuevo art. 44.3.b)–. Aunque antes, la recogida de datos sin tener el consentimiento tácito era considerada una infracción grave del antiguo art. 44.3.d) LOPD, que calificaba como tal tratar los datos de carácter personal con conculcación de los principios y garantías establecidas en la LOPD, una cláusula demasiado general que no respetaba el principio de seguridad jurídica y que ahora ha sido también modificada, limitándola a la conculcación de los principios y garantías establecidas en el art. 4 –nuevo art. 44.3.c)–.

(133) La Agencia Española de Protección de Datos ha señalado que «para recabar este consentimiento en Internet, se considerará válido un procedimiento en el que el usuario tenga una participación activa, de tal forma que, a través de la web, pueda manifestar su voluntad en uno u otro sentido. Para que la ausencia de manifestación de la voluntad del usuario pueda producir alguna consecuencia respecto del tratamiento de sus datos, habrá que haberle advertido expresamente de esta circunstancia,

más de que puede ser revocado en cualquier momento –como señala el art. 17 del Reglamento de desarrollo de la LOPD–, tienen que ir referido a «un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos» –art. 12.1 del Reglamento de desarrollo de la LOPD–. De hecho, el consentimiento informado implica que no puede llevarse a cabo ningún tratamiento de datos personales sin que previamente el afectado sea informado de las previsiones establecidas en el art. 5 de la LOPD. Así, en muchas ocasiones, la prueba del consentimiento es que el interesado haya aceptado previamente a la recogida de datos los términos expresados en el aviso legal o en la política de privacidad. En realidad, la información previa al consentimiento es lo que hace que éste sea también inequívoco. Sin embargo, como hemos señalado anteriormente, en muchas ocasiones, la política de privacidad, el aviso legal o la leyenda informativa no incluyen todas las previsiones establecidas en el art. 5 LOPD. En este caso, la recogida de datos no sólo vulneraría el principio de información sino también el de consentimiento(134). A nuestro juicio, es recomendable por ser más garantista con los derechos de los ciudadanos que los servicios de Administración electrónica establezcan que la manifestación del consentimiento para el tratamiento sea de manera expresa a través de una afirmación específica del afectado –por ejemplo, marcando el interesado una casilla que previamente no esté marcada en el formulario en el que se acceda al servicio de Administración electrónica(135)–. No olvidemos que corresponde al responsable del tratamiento «la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en el derecho» –art. 12.3 del Reglamento–. De hecho, a efectos prácticos la implantación de un modelo de consentimiento expreso no supone una carga adicional para el responsable del tratamiento porque éste tiene necesariamente que probar también el consentimiento tácito, acreditando el cumplimiento de la información previa, expresa, precisa o inequívoca –lo que habitualmente hará conservando el soporte, aunque esto último no sea una obligación legal como ha recordado el Tribunal Supremo–.

Por tanto, es necesario el consentimiento del interesado para la recogida de datos personales para la suscripción en servicios de novedades o de noticias –*newsletter*– o de alertas SMS o MMS o para el tratamiento

así como de los efectos de la misma». Cfr. Recomendaciones de la Agencia de Protección de Datos al sector del comercio electrónico, para la adecuación de su funcionamiento a la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal –accesible en su web–.

(134) Otra cosa distinta es que en el ámbito de un procedimiento administrativo sancionador –que aplica muchas de las garantías del ámbito penal– sólo se declare una de las dos infracciones.

(135) Esta forma de recabar el consentimiento expreso se encuentra prevista en la Recomendación 3/2008 de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica.

de datos personales en foros de discusión(136). En otras ocasiones, las Administraciones Públicas –siguiendo en este punto una práctica de las entidades privadas que facilitan las propias tecnologías de la información– pueden llegar a almacenar datos personales –recurriendo a las denominadas *cookies*– sobre los itinerarios que siguen los ciudadanos al visitar los sitios web de la Administración –qué sitios han sido visitados anteriormente, cuáles posteriormente, cuáles son las secciones que reciben más visitas, cuáles son los documentos más descargados–, tanto para obtener información administrativa como para iniciar trámites con la Administración(137). La finalidad de esta medida es tratar de mejorar la

(136) Únicamente debe darse de alta al ciudadano en un servicio de novedades por email de una Administración cuando da su consentimiento libre, inequívoco, específico e informado para esta finalidad. Además, lo recomendable es que la información al ciudadano se limite al tema que elija y no a todas las noticias posibles. Estas suscripciones a listas de distribución de contenidos deben ser validadas enviando un mensaje a la dirección de correo electrónico del interesado para que confirme su consentimiento. También debe facilitarse en cualquier momento un medio sencillo y gratuito para la revocación del consentimiento. La visita de un ciudadano a un sitio web de la Administración o la realización de solicitudes administrativas por medios electrónicos –por ejemplo, una beca de comedor o una inscripción en una actividad deportiva– no justifican la utilización del correo electrónico para darle de alta en un servicio de novedades. La suscripción a un servicio de noticias electrónicas de una Administración es un servicio de valor añadido que no forma parte de la función administrativa ni de la primera relación negocial o administrativa, por lo que se requiere el consentimiento del interesado. Si bien la Ley de Servicios de la Sociedad de la Información permite el envío de correos de carácter comercial por parte de una empresa con la que se haya mantenido una relación previa, como ya hemos señalado en otro momento, la protección de datos personales es también una garantía del principio democrático, especialmente cuando se quiere utilizar la información personal en poder de las Administraciones Públicas para hacer una actividad de marketing administrativo o político. Cfr. en esta dirección nuestro «Prólogo» a L. REBOLLO y M. SERRANO, *Introducción a la protección de datos*, Dykinson, Madrid, 2008, y la «Introducción y Presentación» a *Protección de datos personales para Administraciones Locales*, Civitas-APDCM, Madrid, 2008, pp. 99-101.

(137) Cfr. J. VALERO TORRIJOS, «El uso de *cookies* por las Administraciones Públicas: ¿una vulneración de la normativa sobre protección de los datos personales?», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 3, 2003, pp. 176-177; e «Implicaciones de la protección de datos de carácter personal para la Administración electrónica», cit., pp. 187-190. La utilización de *cookies* ha sido analizada por el Grupo de Trabajo del Artículo 29 en el documento de trabajo «Privacidad e Internet: enfoque comunitario integrado de la protección de datos en línea», de 21 de noviembre de 2000, pp. 17-18. *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37es.pdf*. Muchos servicios de Administración electrónica almacenan una *cookie* permanente o *tracking cookie* cuando se accede a un sitio web de la Administración. Muchas veces son empresas externas –Nielsen, por ejemplo– las que acceden a la *cookie* y utilizan el identificador único para actualizar la información sobre navegación de la persona. Cuando el usuario accede a cualquier otro sitio web federado –controlado también por la misma empresa–, la compañía reconoce la *cookie* y es capaz de actualizar el historial de navegación con los accesos a todos los sitios web que controla. Esto permite hacer estudios de *marketing* –por ejemplo, del porcentaje de personas que visitan diariamente un servicio de Administración electrónica así como un determinado medio de comunicación–. Este tratamiento de datos personales se hace habitualmente sin declarar el fichero, sin respetar el principio de información, sin el consentimiento del interesado y sin un contrato de encargado de trata-

información que las Administraciones Públicas ofrecen en Internet, e, incluso, dar un servicio más personalizado en una próxima visita al sitio web –enviando un mensaje con las principales novedades desde la última visita, incluso adaptando la información en función de los intereses de cada ciudadano–, lo que contribuye a mejorar la satisfacción de los ciudadanos. En otras ocasiones, se almacena esta información personal por el mero hecho de almacenarla, sin conocimiento de los propios responsables públicos y sin ninguna finalidad evidente. Pues bien, la utilización de *cookies*, como hemos señalado anteriormente, supone un tratamiento de datos personales que debe estar declarado a través de una disposición de carácter general y que debe respetar especialmente el principio de información. Además, a nuestro juicio, la personalización de la información administrativa del sitio web es un servicio de valor añadido del art. 6.3 de la Directiva 2002/58/CE(138) y no supone el ejercicio de una función administrativa por lo que se requiere el consentimiento del interesado(139). Existe un derecho a la información administrativa –art.

---

miento cuando se apoyan en empresas externas –que no pueden tratar los datos para fines propios sino para prestar un servicio al responsable del fichero–. A nuestro juicio, los servidores web de la Administración deben obtener automáticamente el mínimo de información técnica imprescindible para dar un buen servicio. Por ejemplo, en el momento de conexión puede analizarse el tipo de navegador que se está utilizando (Internet Explorer, Mozilla Firefox, etc.) y su versión con el objetivo de seleccionar la hoja de estilo más adecuada y que la visualización del portal sea correcta, así como el idioma y el juego de caracteres de su navegador con el mismo motivo (por ejemplo, para que se vean bien los acentos). La utilización de *cookies* de visita (Nielsen Online) tiene que tener un objeto exclusivamente estadístico (por ejemplo, para conocer el número de "visitantes únicos" que tiene la –web de la Administración– y que contiene un identificador exclusivo y aleatorio que se envía a su navegador desde un servidor web y se almacena posteriormente en el disco duro del ordenador. Por medio de modificaciones en las preferencias del navegador, un visitante puede elegir entre aceptar todas las *cookies*, recibir una notificación cuando se envía una *cookie* o rechazar todas las *cookies*. Si desea desactivar la *cookie*, bien sea totalmente, bien sea de manera anónima, debe poder hacerlo a través de un enlace.

(138) «El proveedor de un servicio de comunicaciones electrónicas disponible para el público podrá tratar los datos a que se hace referencia en el apartado 1 para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido en la medida y durante el tiempo necesarios para tales servicios o promoción comercial, siempre y cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento. Los usuarios o abonados dispondrán de la posibilidad de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento».

(139) Es especialmente importante que las tecnologías incorporen medidas que permitan el derecho del ciudadano a controlar los datos personales que saltan de su terminal, lo que implica el consentimiento para las *cookies*. Ya hemos mencionado la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) –COM (2007) 228 final, de 2 mayo 2007– que menciona como una de las formas de PET «los anuladores de *cookies*, que bloquean las *cookies* introducidas en un ordenador para que lleve a cabo determinadas instrucciones sin que el usuario tenga conocimiento de ello, responden al principio de que los datos deben tratarse de forma lícita y transparente y que ha de informarse al interesado del tratamiento que se realice». Cfr. también el artículo 14.3 de la Directiva 2002/58/CE, de 12 de julio de 2002.

35.g) LRJAP y PAC– que debe desarrollarse en el marco de la atención al ciudadano y que no precisa de identificación, por lo que no debe establecerse esta exigencia para acceder a la información por medios electrónicos –ya que esto supone una discriminación en relación con aquellos que solicitan ésta por teléfono o de manera presencial–(140). En ningún caso sería legítima la exigencia de admitir la *cookie* para poder visitar el sitio web de la Administración ya que ésta está obligada a ofrecer esta información sin necesidad de ninguna identificación. Ya hemos señalado que la LAECSP proclama el principio de igualdad y prohíbe la existencia de discriminaciones para los ciudadanos cualquiera que sea la forma que éstos elijan para relacionarse con la Administración –art. 4.b)–. Por tanto, sólo si existe consentimiento del interesado puede recurrirse a la utilización de *cookies* en los sitios web de la Administración Pública.

Lógicamente el tratamiento de datos de menores de edad sigue sus reglas específicas –art. 13 del Reglamento de desarrollo de la LOPD–(141). Es frecuente los tratamientos de datos de menores en los

(140) El Grupo del Artículo 29 en el documento antes citado sobre Administración en línea ha analizado la retención de datos personales en los portales administrativos. Señala el informe que no se retendrían datos personales en Dinamarca, Alemania, España, Portugal y Suecia. En cambio, pueden o podrán retenerlos en Bélgica, Italia, Noruega, Finlandia, Austria (sólo si el ciudadano está entrando en un procedimiento para el cual sea indispensable que se identifique) e Irlanda. Así, el Decreto 21/2002, de 24 de enero, por el que se regula la atención al ciudadano en la Comunidad de Madrid obliga a informar de los procedimientos administrativos de la Comunidad de Madrid, incluyendo como datos básicos la normativa que los regule, la unidad responsable con su dirección, teléfono y demás medios de comunicación de que disponga, los documentos necesarios para el inicio y tramitación del procedimiento, los trámites a realizar, los plazos y resolución y la necesidad, en su caso, de abono de tasas. Asimismo, dentro de la información general que se ofrece a través de estos medios, se pondrá a disposición de los ciudadanos información sobre todas las subvenciones y ayudas que convoque la Comunidad de Madrid, en la que se incluirán los datos básicos descritos para los procedimientos, destacando visiblemente los plazos, requisitos y medios de información complementarios, e incorporando el impreso normalizado de solicitud que podrá cumplimentarse directamente desde el propio Sistema de Información. Este Decreto 21/2002, de 24 de enero, establece en su artículo 12 que la información que la Comunidad de Madrid ofrece por las redes de Internet e Intranet es parte integrante del Sistema de Información al Ciudadano y se organiza en el sitio web de la Comunidad de Madrid que se configura como el portal de servicios de las diferentes unidades administrativas en su relación con los ciudadanos.

(141) La problemática de los tratamientos de datos personales de menores debe ser abordada desde los diversos ámbitos, teniendo en cuenta la autonomía del menor y la existencia de una legislación sectorial que modula la asistencia de los titulares de la patria potestad. Cfr. nuestra «Introducción y Presentación» a *Protección de datos personales para Servicios Sanitarios Públicos*, pp. 102-115, a *Protección de datos personales para Servicios Sociales Públicos*, pp. 51-54, a *Protección de datos personales para Universidades*, pp. 66-73, y a *Protección de datos personales para centros educativos públicos*, pp. 61-64 y pp. 81-86 –todos ellos editados conjuntamente por Civitas-APDCM en el año 2008–. La protección de los menores en las redes sociales en Internet es una cuestión que hemos abordado en «Redes sociales y protección de datos personales», un trabajo que se publicará próximamente en un libro dirigido por J. L. Piñar Mañas. Cfr. también una referencia a la titularidad y al ejercicio de los menores del derecho fundamental a la protección de

servicios de Administración electrónica –para la participación en un foro electrónico, para la emisión del carné de biblioteca, para el uso de instalaciones deportivas, para inscribirse en un curso municipal, etc–. Puede procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento salvo que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela, debiendo cumplirse el principio de información con un lenguaje que le sea fácilmente comprensible. Es necesario, como señala el art. 13.4 del Reglamento de desarrollo de la LOPD, que el responsable del fichero «articule los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado, en su caso, por los padres, tutores o representantes legales», una previsión que ha sido expresamente respaldada en la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de julio de 2010 –Sección Sexta–(142).

---

datos personales en A. TRONCOSO REIGADA, «La protección de los datos sanitarios del menor», en *Nuevos retos que plantean los menores al Derecho*, Universidad Pontificia de Comillas, Madrid, 2004, pp. 213-222.

(142) El art. 13.4 del Reglamento fue también objeto de impugnación ante el Tribunal Supremo por la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) al entender que el precepto imponía una obligación «ex novo» no prevista en la LOPD ni en la Directiva 95/46/CE, y que esta obligación era de difícil o de imposible cumplimiento y desproporcionada. Señalaba también el recurrente que la Directiva 95/46/CE debía ser interpretada de conformidad con el principio del interés superior del menor, que este interés en muchas ocasiones no coincide con el de sus representantes, que hay supuestos en que el tratamiento de datos personales era legítimo sin contar con el consentimiento del menor y que además se ha de tener en cuenta su grado de madurez. Los recurrentes incluían una serie de interrogantes relativos a la posibilidad de representación voluntaria para el tratamiento de datos de menores, a la necesidad de establecer garantías sobre la autenticidad de esa representación, a la forma de resolver un hipotético conflicto de intereses entre el menor y sus representantes legales, y a si debe resolverlo el responsable del fichero o del tratamiento. Como señala acertadamente la Sentencia –Fundamento Jurídico 8º–, no se entiende la razón de la impugnación ya que el art. 13 del Reglamento no limita los supuestos en que conforme a la Directiva 95/46/CE o la LOPD no es necesario el consentimiento para el tratamiento sino que se circunscribe a establecer la posibilidad del consentimiento para el tratamiento por parte de los mayores de catorce años, salvo que la Ley exija para su prestación la asistencia de los titulares de la patria potestad, una previsión que remite a la legislación específica y que es respetuosa con la legislación de autonomía del menor y con las previsiones en la legislación sectorial, especialmente en el ámbito sanitario y de servicios sociales –como hemos analizado en los trabajos citados en la nota anterior–. La posibilidad de que existan conflictos de intereses entre el menor y el representante legal es objeto de regulación en los arts. 162 y 163 del Código Civil y no puede ser abordado por Reglamento. El Reglamento se limita a recordar la obligación que tiene el responsable del tratamiento de comprobar el cumplimiento de esa edad y la autenticidad del consentimiento prestado por los padres, tutores o representantes legales, en garantía de futuras demandas de nulidad. Como señala la Sentencia, «cierto es que la comprobación de la edad del menor puede presentarse en ocasiones como difícil, pero ello no debe de servir de excusa para la adopción de las medidas de garantía adecuadas que, en definitiva, es lo único que exige el precepto reglamentario impugnado, razón esta última que impide considerar la exigencia que previene como desproporcionada, cuando afecta o incide en un ámbito especialmente sensible».

Por último, hay que señalar que si el tratamiento en el ámbito de la Administración electrónica se sustancia sobre datos especialmente protegidos no es suficiente el consentimiento tácito sino que es necesario también un consentimiento expreso –para los datos de raza, salud y vida sexual– y un consentimiento expreso y escrito –para los datos de ideología, afiliación sindical, religión o creencias–, con expresa advertencia del derecho a no prestarlo –art. 7 LOPD–. La LOPD exceptúa el consentimiento en el tratamiento de los datos especialmente protegidos cuando dicho tratamiento sea necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o los tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento se realice por un profesional sanitario sujeto a secreto profesional o por otra persona sujeta a una obligación idéntica de secreto –art. 7.6–, al mismo tiempo que permite el tratamiento de los datos de carácter personal relativos a la salud de las personas que acudan a centros sanitarios públicos o privados o hayan de ser tratados en los mismos –art. 8–. Por tanto, no es necesario el consentimiento del interesado para la implementación de proyectos como la historia clínica electrónica o la receta electrónica, lo que no implica, como ya hemos aclarado antes, una obligación de los ciudadanos de comunicarse con la Administración por medios electrónicos. En todo caso, los tratamientos de datos especialmente protegidos que lleve a cabo la Administración y que se desarrollen sin consentimiento del interesado tienen que ser muy cuidadosos con el respeto a otros principios como el de calidad –evitando datos excesivos que provengan de apreciaciones subjetivas de los profesionales si no son imprescindibles para la finalidad– y el de información(143).

V. LAS COMUNICACIONES DE DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA

1. EL CONSENTIMIENTO DEL INTERESADO Y LA HABILITACIÓN LEGAL

Mención específica merece las comunicaciones de datos entre Administraciones Públicas –accesos electrónicos e interconexiones–, algo consustancial a la Administración electrónica. Como señala el Grupo de Trabajo del Artículo 29(144), «podemos observar el desarrollo de diferentes tipos de proyectos de administración en línea que consisten en la creación y la promoción del suministro de procedimientos administrativos en línea. El éxito de algunos de ellos depende de complejas cuestiones

(143) Cfr. A. TRONCOSO REIGADA, «Introducción» a *Principios y derechos de protección de datos personales. Doctrina de la Agencia de Protección de Datos de la Comunidad de Madrid 2002-2009*, cit., pp. 154-159.

(144) Cfr. la «Introducción» del Documento de trabajo sobre la administración en línea, de 29 de enero de 2003, ya citado.

relacionadas con la protección de datos que se habrán de estudiar atentamente. A título de ejemplo podemos mencionar el establecimiento de puntos de entrada únicos a los servicios de administración en línea, la creación de identificadores únicos y la interconexión de las bases de datos públicas». Las ventajas para el ciudadano –sobre todo de comodidad– dimanantes de la comunicación de datos entre Administraciones Públicas que evita la presentación de determinados documentos se pueden convertir en perjuicios si esto supone una interconexión generalizada de bases de datos públicas que, dada la cantidad ingente de información, no sólo establecen perfiles de las personas sino que afectan a la intimidad, al libre desarrollo de la personalidad y al ejercicio de otros derechos fundamentales, sustituyendo el control sobre la propia información personal por un control de la Administración sobre los individuos. De hecho, la Sentencia del Tribunal Supremo Alemán sobre la Ley del Censo que reconoce el derecho a la autodeterminación informativa lo hace en relación con las interconexiones(145). Piénsese, por ejemplo, en una información ofrecida voluntariamente por una persona a una Administración para obtener una prestación social que se emplea por otra para limitar otros derechos.

La Ley Orgánica de Protección de Datos establece que los datos de carácter personal sólo 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 –art. 11.1 LOPD–. La LOPD establece un régimen de excepciones en los arts. 11 y 21, entre las que destaca, entre otras, que la cesión esté autorizada por Ley –art. 11.2.a) LOPD–. En virtud de esta legislación de protección de datos personales es posible la comunicación de datos entre Administraciones Públicas por medios electrónicos con el consentimiento del interesado –que también puede ser expresado por medios electrónicos– o la presencia de una habilitación legal –cuando exista un interés público–. La legislación española relativa a la Administración electrónica siempre ha exigido que el acceso y la interconexión de datos entre Administraciones Públicas se hagan sólo con el consentimiento del interesado o a través de una habilitación legal(146). Así, una Administración –Ayuntamiento, Seguridad Social, Agencia Tributaria– sólo podrá comunicar

(145) El Grupo de Trabajo del Artículo 29 en el documento antes citado recoge que la Autoridad británica ha prestado un interés especial en que la Administración en línea no funcione como una pantalla de humo que oculte una interconexión generalizada de las bases de datos de información pública y un mayor intercambio de datos personales entre Administraciones. Igualmente, en su informe para el gobierno francés sobre la Administración en línea y la protección de los datos personales, la CNIL recordó también su doctrina consistente en rechazar una interconexión generalizada de los ficheros. Para la CNIL, la Administración en línea no debería suponer un aumento del control ejercido sobre los individuos, que derivaría principalmente de las interconexiones.

(146) La normativa –alguna de ella ya derogada– ha insistido en el consentimiento del interesado para la comunicación de datos entre Administraciones Públicas. En esta dirección hay que señalar que la Disposición Adicional decimoctava de la LRJ-PAC –añadida por el art. 68.3 de la Ley

datos –de empadronamiento, tributarios, de no tener deudas con la segu-

24/2001, de 28 de diciembre y derogada por la LAECSP– en relación con la solicitud de certificaciones tributarias y de Seguridad Social cuando deban aportarse a otros procedimientos administrativos, establecía que «[l]a aportación de certificaciones tributarias o de Seguridad Social junto con las solicitudes y comunicaciones a que se refieren los apartados anteriores se sustituirá, *siempre que se cuente con el consentimiento expreso de los interesados*, por la cesión de los correspondientes datos al órgano gestor por parte de las Entidades competentes». También se señala que «[l]o dispuesto en la presente disposición se ajustará a lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en la presente Ley, en la vigente normativa sobre firma electrónica y en las correspondientes normas de desarrollo». Así, la legislación exigía el consentimiento expreso para la comunicación, aunque ésta se enmarque en un procedimiento que suponga un beneficio para el afectado. Si no existe este consentimiento, el propio afectado debía aportar estas certificaciones. Igualmente, la Disposición adicional cuarta de la Ley 40/1998, de 9 de diciembre, Reguladora del Impuesto sobre la Renta de las Personas Físicas –que conserva su vigencia en virtud del Real Decreto Legislativo 3/2004, de 5 de marzo– establece lo siguiente: «*Previa autorización de los interesados* y en los términos y con las garantías que se establezcan mediante orden del Ministro de Economía y Hacienda, la información de carácter tributario que precisen las Administraciones Públicas para el desarrollo de sus funciones podrá ser suministrada a aquéllas directamente por la Agencia Estatal de Administración Tributaria por medios informativos o telemáticos, en el marco de colaboración que se establezca. Asimismo, en la Orden citada se podrá regular el suministro de información en los casos previstos en el artículo 113.1 de la Ley 230/1963, de 28 de diciembre, General Tributaria. En la medida en que a través del indicado marco de colaboración las Administraciones Públicas puedan disponer de dichas informaciones no se exigirá a los interesados que aporten individualmente certificaciones expedidas por la Agencia Estatal de Administración Tributaria, ni la presentación, en original, copia o certificación, de sus declaraciones tributarias». El Real Decreto 209/2003, de 21 febrero, por el que se regulaba los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos, introduce en su art. 2 una modificación del Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado estableciendo –nuevo art. 14.2– que «[l]a expedición de un certificado telemático se realizará: a) A solicitud del interesado, a quien le será enviado o puesto a disposición para su remisión al órgano que lo requiere. *b) A instancia del órgano requirente, bien a iniciativa del interesado, o del propio órgano requirente, siempre que cuente con el expreso consentimiento de aquél*, salvo que el acceso esté autorizado por una ley. En este supuesto, la petición de certificado identificará el trámite o procedimiento para el que se requiere y *hará constar que se dispone del consentimiento expreso del interesado* o la norma que lo exceptúe». Asimismo, se indica que «A estos efectos, el consentimiento del interesado para que el certificado sea requerido por el órgano tramitador del procedimiento habrá de constar en la solicitud de iniciación del procedimiento o en cualquier otra comunicación posterior, sirviendo el recibo de presentación de ésta como acreditación del cumplimiento del requisito de presentación del certificado». El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio ha derogado el Real Decreto 263/1996, de 16 de febrero.En la misma dirección, el Real Decreto 523/2006, de 28 de abril, por los que se suprime la exigencia de aportar el certificado de empadronamiento, como documento probatorio del domicilio y residencia, en los procedimientos tramitados por la Administración General del Estado y por sus organismos públicos vinculados o dependientes parte del consentimiento del interesado para evitarle aportar un documento que ya está en poder de la Administración. Así, señala expresamente que «será preciso *el consentimiento del intensad*o para que los datos puedan ser consultados por este sistema por el órgano instructor, debiendo constar dicho consentimiento en la

ridad social, etc.– a otra Administración responsable de la tramitación de un procedimiento con el consentimiento –en muchas ocasiones se ha pedido que fuera expreso– o la previa autorización del interesado, salvo que exista una habilitación legal. Así, se ha afirmado que si el interesado no prestara su consentimiento deberá aportar directamente la certificación correspondiente de la otra Administración, siendo la no aportación de esta certificación la causa para requerirle la subsanación de conformidad con el art. 71.1 de la LRJAP y PAC.

La LAECSP reconoce el derecho «[a] no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados(147). El citado consentimiento podrá emitirse y recabarse por medios electrónicos» –art. 6.2.b)–(148). La LAECSP ha mantenido, pues,

---

solicitud de iniciación del procedimiento o en cualquier otra comunicación posterior. A tal efecto, la *prestación del consentimiento del interesado* podrá hacerse constar expresamente en el recibo de presentación de su solicitud. En cualquier caso, si el interesado no prestara su consentimiento deberá aportar el certificado de empadronamiento, siendo la no aportación de aquél causa para requerirle la subsanación de conformidad con el art. 71.1 de la LRJ-PAC». Así, establece la propia Exposición de Motivos que «[s]erá el órgano administrativo responsable de la tramitación de dicho procedimiento el que deba, con *el previo consentimiento del interesado*, consultar las propias bases de datos de la Administración General del Estado, a fin de comprobar los datos de domicilio proporcionados por el ciudadano en su solicitud. Cuando el ciudadano no figure en sus bases o los datos de domicilio no sean coincidentes, el propio órgano administrativo solicitará el certificado de empadronamiento al Ayuntamiento correspondiente». El art. 5.3 del Reglamento Técnico del Sistema de Verificación de Datos de Residencia, aprobado por la Orden PRE/4008/2006, de 27 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema, señala que no podrá realizarse consulta alguna en caso de no contar con el consentimiento del interesado de forma fehaciente. Algo semejante puede decirse del Real Decreto 522/2006, de 28 de abril, por el que se suprime la exigencia de aportación de la fotocopia del DNI en los procedimientos tramitados por la Administración General del Estado y sus organismos vinculados o dependientes.

(147) La excepción que establece el art. 6.2.b) relativa a que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados hace referencia principalmente a la regulación sobre materias clasificadas como secreto.

(148) La Exposición de Motivos de la LAECSP establece que este consentimiento tiene que ser expreso –adpo. VI–. Esto, además de no ser una obligación establecida en la LOPD, no ha sido seguido por el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, que ha previsto el consentimiento tácito. El Anteproyecto de la LAECSP exigía el consentimiento expreso pero la tramitación en el Congreso de los Diputados suprimió el carácter de expreso, señalando que el consentimiento será en los términos establecidos en la LOPD. Si bien la LAECSP podía haber exigido el carácter expreso del consentimiento –con la finalidad de ser más garantista–, el legislador prefirió finalmente no modificar la regulación del consentimiento para el tratamiento que se contenía en la LOPD,

este régimen de consentimiento o norma con rango de Ley(149). De esta forma, el intercambio de certificados y la transmisión de datos personales entre Administraciones Públicas distintas requiere la existencia de una norma con rango de ley o la presencia del consentimiento del interesado –o bien que el ciudadano obtenga el certificado de manera telemática y se lo facilite a la Administración, aunque en este caso no estaremos hablando realmente de comunicación de datos entre Administraciones Públicas–(150). La LAECSP no ha querido modificar el régimen de cesiones

---

incluyendo una remisión a la misma. Una enmienda del Grupo popular –que fue desestimada– propuso introducir la exigencia del principio de calidad dentro de este precepto de manera que la información que se recabase de otras Administraciones Públicas quedase «estrictamente limitada al contenido de la relación jurídica con los interesados». Cfr. L. COTINO HUESO, «Derechos del ciudadano», cit., pp. 192-193.

(149) A esta cuestión también se ha referido el documento ya citado el Grupo del Artículo 29 sobre Administración en línea, de 29 de enero de 2003, que señala: «una primera tendencia a la que varios países se adhieren expresamente, generalmente apoyados por sus autoridades de protección de datos (Irlanda, Dinamarca, España, Finlandia), consiste en considerar que los ciudadanos deben mantener sus datos bajo control en todas las fases de los procedimientos administrativos y que se les debe informar de los intercambios de datos correspondientes a las decisiones que se han tomado acerca de ellos. Como consecuencia de esta tendencia, el intercambio de datos entre administraciones por medios telemáticos se puede ver sujeto al consentimiento de los afectados (por ejemplo, en España e Irlanda). En otros países (Reino Unido, Bélgica) la situación es más vacilante. Esta primera tendencia se ve respaldada por la idea de que tal control personal condicionaría la confianza que debe generar la administración en línea, así como su credibilidad. Del mismo modo, cuanto más confíen los ciudadanos en su administración, menos necesitarán ejercer tal control […]. En cambio, se recomienda y acepta que se dé a los ciudadanos una oportunidad de consentir su inclusión en el nuevo sistema y que se les informe acerca de los fines y usos de la base de datos central. […]. El individuo deberá decidir con libertad qué datos adicionales facilita para disponer de un conjunto de servicios más amplio. Del mismo modo, los individuos han de ser conscientes del abanico de usos potenciales de sus datos en el momento de su recogida […]».

En cuanto a la segunda tendencia, consiste en considerar que la simplificación administrativa exige necesariamente cierta pérdida de control de los datos personales por parte del usuario. De este modo, no se podrán satisfacer al mismo tiempo las exigencias relativas a una mayor rapidez de la administración en línea y las relativas al suministro «tradicional» de información a los ciudadanos. Tres países (Portugal, Alemania e Italia) consideran que el control de los ciudadanos sobre sus datos no es una consecuencia necesaria del desarrollo de la administración en línea. Un argumento que la Autoridad francesa plantea a este respecto es el riesgo de que en la práctica ese control no sea más que una ilusión. El usuario podría pensar, erróneamente, que controla sus datos, pero en realidad es evidente que la ley y los reglamentos pueden obligar a los individuos a facilitar datos a la administración. En esta misma línea, la Autoridad portuguesa de protección de datos considera que, aunque la administración en línea pueda soportar parcialmente el derecho de la persona a acceder a sus datos disponibles en línea, el usuario no ejercerá ningún control suplementario sobre sus datos, especialmente en relación con el consentimiento del titular a comunicarlos a terceras partes dentro de la administración».

(150) Cfr. sobre la cuestión –con un planteamiento distinto al nuestro– Mª DEL MAR PÉREZ, «La regulación jurídica de la interconexión de bases de datos personales en el contexto de la Administración Electrónica», *Datospersonales.org Revista de la Agencia de Protección de Datos de la Comunidad de Madrid* nº 12, 2004 para quien «la generalización del consentimiento de la persona concernida parece una garantía totalmente

de datos entre Administraciones Públicas para implantar la Administración electrónica, a pesar de ser una ley y como tal tener el rango suficiente para limitar derechos fundamentales y para establecer un régimen más flexible de cesiones. Así, a pesar de que el art. 9 de la LAECSP establece un deber de cooperación entre Administraciones Públicas para permitir el acceso a los datos relativos a los interesados que obren en su poder, en ningún momento establece una cláusula abierta que permita las transmisiones de datos entre Administraciones Públicas distintas a las previstas en el art. 6.2.b) de la LAECSP sino que al contrario señala que «el acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b) de la presente Ley» (151). Sí es importante mencionar una pequeña diferenciación entre la previsión contenida en el art. 35.f) de la LRJAP y PAC y aquella recogida en el art. 6.2.b) de la LAECSP. La primera reconoce el derecho «a no presentar documentos no exigidos por las normas aplicables al procedimiento de que se trate o que ya se encuentren en poder de la Administración actuante» –art. 35.f) LRJAP y PAC–; en cambio la segunda reconoce el derecho «[a] no aportar los datos y documentos que obren en poder de las Administraciones Públicas, *las cuales utilizarán medios electrónicos para recabar dicha información*» –art. 6.2.b) LAECSP–, lo que tiene consecuencias también en relación con el consentimiento tácito.

2. TRES SUPUESTOS DE CONSENTIMIENTO TÁCITO: EL DERECHO A NO APORTAR DATOS Y DOCUMENTOS QUE OBREN EN PODER DE LAS ADMINISTRACIONES PÚBLICAS; LAS COMPROBACIONES DE LAS COPIAS DIGITALES DE LOS DOCUMENTOS APORTADOS POR LOS CIUDADANOS Y LA VERIFICACIÓN DE LA AUTENTICIDAD DE LOS DATOS PERSONALES CONTENIDOS EN LAS SOLICITUDES QUE SE DIRIGEN A LA ADMINISTRACIÓN. LA PROBLEMÁTICA DEL FORMULARIO PREVIAMENTE CUMPLIMENTADO

Recientemente el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, ha regulado las transmisiones de datos y documentos, incluidos certificados,

---

insuficiente en ausencia de una regulación equilibrada y general de las interconexiones de bases de datos». Esta autora plantea interesantes propuestas en su trabajo que no pueden ser abordadas en esta ocasión.

(151) Es este artículo 6.2.b) de la LAECSP el que regula las condiciones que permiten las transmisiones de datos entre Administraciones Públicas, además de las previsiones establecidas en los arts. 11 y 21 de la LOPD. Así, el art. 9 de la LAECSP establece un deber de cooperación entre Administraciones Públicas para permitir el acceso a los datos relativos a los interesados que obren en su poder, estableciendo unas exigencias relativas al principio de seguridad –en su primer apartado– y al principio de calidad y proporcionalidad –en su segundo apartado–. En ningún momento el art. 9 de la LAECSP autoriza transmisiones de datos entre Administraciones Públicas distintas a las previstas en el art. 6.2.b) de la LAECSP.

entre órganos y organismos de la Administración General del Estado que tratan de materializar el ejercicio del derecho reconocido en el art. 6.2.b de la LAECSP a no aportar datos y documentos que obren en poder de las Administraciones Públicas, estableciendo un conjunto de reglas –art. 2–: la primera, que los interesados deben ser informados expresamente de que el ejercicio del derecho implica su consentimiento para que el órgano y organismo ante el que se ejercita pueda recabar los datos o documentos respecto de los que se ejercita el derecho ante los órganos u organismos en que los mismos se encuentren; la segunda, que el derecho se ejercitará de forma específica e individualizada para cada procedimiento concreto, sin que el ejercicio del derecho ante un órgano u organismo implique un consentimiento general referido a todos los procedimientos que aquél tramite en relación con el interesado; tercero, que los interesados en cualquier momento podrán revocar su consentimiento para el acceso a datos de carácter personal así como aportar los datos, documentos o certificados necesarios(152); cuarto, que los órganos u organismos ante los que se ejercite el derecho conservarán la documentación acreditativa del efectivo ejercicio del derecho incorporándola al expediente en que el mismo se ejerció. Esta documentación estará a disposición del órgano cedente y de las autoridades a las que en su caso corresponda la supervisión y control de la legalidad de las cesiones producidas. Esta regulación es distinta de la previsión que se contenía Disposición Adicional decimoctava de la LRJAP y PAC –añadida por el art. 68.3 de la Ley 24/2001, de 28 de diciembre y derogada por la LAECSP– que permitía la sustitución de las certificaciones tributarias o de Seguridad

(152) Este artículo también establece que «si el órgano administrativo encargado de la tramitación del procedimiento, posee, en cualquier tipo de soporte, los datos, documentos o certificados necesarios o tiene acceso electrónico a los mismos, los incorporará al procedimiento administrativo correspondiente sin más trámite. En todo caso, quedará constancia en los ficheros del órgano u organismo cedente del acceso a los datos o documentos efectuado por el órgano u organismo cesionario. Cuando el órgano administrativo encargado de la tramitación del procedimiento no tenga acceso a los datos, documentos o certificados necesarios, los pedirá al órgano administrativo correspondiente. Si se tratara de un órgano administrativo incluido en el ámbito de aplicación del art. 1.2ª) del Real Decreto deberá ceder por medios electrónicos los datos, documentos y certificados que sean necesarios en el plazo máximo que establezca la normativa específica, que no podrá exceder de diez días. Dicho plazo máximo será igualmente aplicable si no está fijado en la normativa específica. […]. En caso de imposibilidad de obtener los datos, documentos o certificados necesarios por el órgano administrativo encargado de la tramitación del procedimiento se comunicará al interesado con indicación del motivo o causa, para que los aporte en el plazo y con los efectos previstos en la normativa reguladora del procedimiento correspondiente». La redacción de este precepto puede dejar entrever que existen cesiones dentro del ámbito de la misma persona jurídica cuando, desde nuestra posición, las únicas cesiones dentro del ámbito de aplicación del Real Decreto se producirían entre las Administraciones Institucionales y la Administración General del Estado ya que dentro de esta última lo más adecuado sería hablar de accesos vinculados al principio de calidad. Ésta es una cuestión que hemos analizado en «El principio de calidad de los datos», *loc. cit.*, pp. 382-394.

Social por la comunicación de datos entre las Administraciones Públicas competentes, siempre que se obtenga el consentimiento expreso de los interesados. También la Disposición adicional cuarta de la Ley 40/1998, de 9 de diciembre, Reguladora del Impuesto sobre la Renta de las Personas Físicas establecía la comunicación de datos de naturaleza tributaria entre Administraciones Públicas por medios electrónicos siempre que se contara con la autorización de los interesados. El cambio viene de que la regulación anterior a la LAECSP exige un consentimiento expreso o una autorización expresa para la comunicación de datos por medios electrónicos entre Administraciones Públicas, mientras que el Real Decreto 1671/2009, de 6 de noviembre, considera que el consentimiento exigido por la LAECSP para que el derecho a no aportar documentos que obren en poder de la Administración se convierta en una comunicación de datos entre Administraciones Públicas viene del propio ejercicio del derecho, que implica el consentimiento para que el organismo ante el que se ejercita pueda recabar los datos o documentos respecto de los que se ejercita el derecho, siempre y cuando los interesados sean informados expresamente y previamente de este hecho. Parece evidente que si para presentar una solicitud a la Administración hace falta aportar certificaciones y documentos de otras Administraciones Públicas y yo me acojo al derecho que no es a «no aportar datos o documentos administrativos que obren en poder de las Administraciones Públicas» sino a no aportar los datos y documentos que estén en poder de las Administraciones Públicas *«las cuales utilizarán medios electrónicos para recabar dicha información»* –art. 6.2.b) LOPD–, estoy dando mi consentimiento para la cesión siempre que disponga de una información previa, expresa, precisa e inequívoca. Si bien es verdad que la previsión del art. 2 del Real Decreto 1671/2009, de 6 de noviembre, por la que se desarrolla parcialmente la LAECSP es algo distinta de la que se contiene en el art. 6.2.b) de la LAECSP, hay que tener en cuenta que este último precepto transcribe en este punto la regulación contenida en la LOPD que no se limita a establecer las cesiones en virtud del consentimiento sino también por habilitación de una norma con rango de ley. Ha sido el Real Decreto 1671/2009, de 6 de noviembre, que desarrolla parcialmente esta Ley el que ha plasmado la forma de manifestar el consentimiento, que va a ser de una manera tácita, pero que sigue siendo libre, inequívoco, específico e informado(153).

(153) Un buen ejemplo de lo que estamos diciendo es el procedimiento de solicitud de subvenciones. La Ley 38/2003, de 17 de noviembre, General de Subvenciones en su art. 23 establece que el procedimiento de subvenciones se inicia de oficio mediante la convocatoria del órgano competente para su concesión, con indicación de los requisitos para solicitar la subvención y la forma de acreditarlos, así como de los documentos e informaciones que deben acompañar a la petición, todo ello con indicación expresa de la disposición que establezca las bases reguladoras de la subvención. El art. 23.3 señala que «las solicitudes de los interesados acompañarán los documentos e informaciones determinados en la norma o convocatoria, *salvo que los documentos exigidos ya estuvieran en poder de cualquier órgano de la Administración actuante, en cuyo caso el solicitante podrá acogerse a lo establecido en el párrafo f del artículo 35 LRJ-PAC*, siempre que se haga constar la fecha y el órgano o dependencia en que fueron presentados o, en su

caso, emitidos, y cuando no hayan transcurrido más de cinco años desde la finalización del procedimiento al que correspondan. En los supuestos de imposibilidad material de obtener el documento, el órgano competente podrá requerir al solicitante su presentación, o, en su defecto, la acreditación por otros medios de los requisitos a que se refiere el documento, con anterioridad a la formulación de la propuesta de resolución. La presentación telemática de solicitudes y documentación complementaria se realizará en los términos previstos en la disposición adicional decimoctava de la LRJ-PAC. A los efectos de lo previsto en el apartado 3 de la citada disposición adicional decimoctava, *la presentación de la solicitud por parte del beneficiario* [de no presentar documentos que estén en poder de la Administración] *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». Hay que señalar que esta Disposición adicional decimo octava –que ha sido derogada por la LAECSP– no dice exactamente que la presentación de la solicitud suponga la autorización sino que señala que «[l]a aportación de certificaciones tributarias o de Seguridad Social junto con las solicitudes y comunicaciones a que se refieren los apartados anteriores se sustituirá, *siempre que se cuente con el consentimiento expreso de los interesados*, por la cesión de los correspondientes datos al órgano gestor por parte de las Entidades competentes».

Sin embargo, si bien la LAECSP en su art. 6.2.b) habla de un consentimiento del interesado, el Real Decreto 1671/2009, de 6 de noviembre que desarrolla parcialmente esta Ley ha señalado en el art. 2 que el ejercicio del derecho a no aportar datos o documentos que estén en poder de otras Administraciones Públicas para que sean éstas las que los reclamen por medios electrónicos implica su consentimiento para la comunicación de datos y documentos desde los órganos en que los mismos se encuentren, siempre y cuando los interesados sean informados expresamente. De esta forma esta regulación es semejante a la prevista en el art. 23 de la Ley de Subvenciones que establece que la solicitud por parte del beneficiario de acogerse a la previsión del art. 35.f) de la LRJ-PAC a no presentar datos o documentos que ya se encuentren en poder de la Administración conlleva 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, lógicamente debiendo añadirse la necesidad de que exista una información expresa y previa de que la solicitud supone el consentimiento para la cesión, la limitación para que sea sólo para ese procedimiento y la posibilidad de revocación por parte del interesado.

El Real Decreto 887/2006, de 21 de julio, por el que se aprueba el Reglamento de la Ley 38/2003, de 17 de noviembre, General de Subvenciones establece en su art. 22 que el cumplimiento de las obligaciones tributarias y con la Seguridad Social se acreditará mediante la presentación por el solicitante ante el órgano concedente de la subvención de las certificaciones correspondientes que serán expedidas por el órgano competente a instancia del interesado en un plazo no superior a 20 días. Estas certificaciones se emitirán preferentemente por medios electrónicos, informáticos o telemáticos. Especialmente se indica –apdo. 4– que *«cuando las bases reguladoras así lo prevean, la presentación de la solicitud de subvención conllevará la autorización del solicitante para que el órgano concedente obtenga de forma directa la acreditación de las circunstancias previstas en los artículos 18 y 19 de este Real Decreto a través de certificados telemáticos, en cuyo caso el solicitante no deberá aportar la correspondiente certificación. No obstante, el solicitante podrá denegar expresamente el consentimiento, debiendo aportar entonces la certificación en los términos previstos en los apartados anteriores»*. Como puede verse, este Real Decreto 887/2006, de 21 de julio, no se limita a prever que cuando el ciudadano ejerza el derecho a no aportar datos y documentos en poder de las Administraciones Públicas para que sean éstas las que utilicen los medios electrónicos para recabar dicha información está consintiendo en la comunicación de datos entre Administraciones Públicas. Este Real Decreto 887/2006, de 21 de julio, da un paso más al establecer que las bases reguladoras pueden prever que la

Así, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, contiene distintos elementos que permiten afirmar la existencia de un consentimiento tácito para la cesión: el cumplimiento del principio de información expresa, inequívoca –está referida a un procedimiento específico e individualizado–, y previa sobre la cesión, que, lógicamente tiene que incluir los contenidos del art. 5 de la LOPD –información precisa de la finalidad del nuevo tratamiento, de la identidad y dirección del responsable y del resto de los extremos incluidos en ese precepto, salvo que se deduzca claramente de la naturaleza de los datos y de las circunstancias en que se recaban–; la posibilidad de revocar en cualquier momento el consentimiento para el acceso de conformidad con el art. 11.4 de la LOPD, que señala que el consentimiento para la cesión es revocable–; y la necesidad de acreditar el cumplimiento del deber de información que, en este supuesto, también lo es de la existencia de un consentimiento tácito, al establecer que los órganos administrativos deberán conservar la documentación acreditativa del efectivo ejercicio del derecho incorporándola al expediente en que el mismo se ejerció, de manera que esté a disposición del órgano cedente y de la autoridad de control(154).

---

presentación de una solicitud de subvención conlleva la autorización del solicitante para que el órgano concedente obtenga de forma directa la acreditación, aunque el ciudadano no se haya acogido todavía al derecho previsto en el art. 6.2.b) de la LAECSP de no aportar una documentación de manera que la recabe electrónicamente la Administración. En todo caso, se podría decir que existe un consentimiento tácito para esta comunicación ya que está prevista en las bases reguladoras, siempre y cuando, como ya hemos señalado anteriormente, se cumplan las previsiones establecidas en el art. 2 del Real Decreto 1671/2009, de 6 de noviembre, especialmente que se haya respetado el principio de información expresa y previa al interesado de la comunicación, que se limite a un procedimiento determinado y que exista la posibilidad de revocación. De alguna manera, el apartado 4 del Real Decreto 887/2006, que permite al solicitante «denegar expresamente este consentimiento» hace referencia a la existencia de un consentimiento tácito. Además, en este supuesto, podría afirmarse también la existencia de una habilitación legal en virtud de la propia Ley de subvenciones, que sería una Ley especial y que encajaría dentro del art. 11.2.a) de la LOPD. Muchas órdenes ministeriales y de consejerías de las Comunidades Autónomas que convocan subvenciones señalan que en caso de no aportarse certificados de estar al corriente de las obligaciones contraídas con la Agencia Tributaria y la Seguridad Social, esta información pueda ser recabada por la propia Administración que convoca las becas, con el consentimiento expreso del afectado. En todo caso, como hemos apuntado en otro momento, si una orden de convocatoria, en virtud de lo establecido en el Real Decreto 887/2006, de 21 de julio, por el que se aprueba el Reglamento de la Ley 38/2003, de 17 de noviembre, General de Subvenciones, afirma expresamente que en el caso de que los certificados de estar al corriente de las obligaciones tributarias no sean aportados por el interesado, puedan ser solicitados de oficio por la propia Administración, podría entenderse que existe un consentimiento tácito. También puede valorarse la aplicación de la excepción al consentimiento prevista en el art. 11.2.c) de la LOPD ya que el tratamiento responde a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. Sobre esta cuestión volveremos más adelante.

(154) Esta obligación de soporte documental que el Real Decreto 1671/2009, de 6 de noviembre, que desarrolla la LAECSP

Otro supuesto distinto es la posibilidad que tiene la Administración de llevar a cabo comprobaciones –automatizadas o no– de las copias digitalizadas de documentos aportadas por los ciudadanos, lo que supone una comunicación de datos entre Administraciones Públicas aunque ejerzan competencias diferentes. La LAECSP, después de afirmar que los interesados podrán aportar al expediente copias digitalizadas de los documentos, señala que «[l]a Administración Pública podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas […]. La aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos» –art. 35–(155). El legislador entiende que la aportación a un expediente de una copia digitalizada «implica la autorización a la Administración para que acceda y trate la información personal», por lo que existiría en este caso un consentimiento tácito del interesado. La comunicación de datos personales para proceder a la verificación de las copias digitalizadas dispondría también de la habilitación legal exigida en el art. 11.2.a) de la LOPD(156). No obstante, es necesario garantizar también al interesado la información previa, expresa, precisa e inequívoca de lo establecido en el art. 5 de la LOPD, señalando claramente que la aportación por parte de éste de una copia digitalizada de un documento implica la autorización para que la Administración Pública destinataria lleve a cabo las comprobaciones sobre la autenticidad de la copia digitalizada aportada.

Un supuesto aún más complejo es la posibilidad que tiene la Administración de llevar a cabo una comprobación de la autenticidad de los datos personales contenidos en las solicitudes que se dirigen a ésta y que obran en poder de otras Administraciones Públicas. No se trata en este caso de que el ciudadano autorice a la Administración para que recabe

---

ha establecido para que los órganos ante los que se ejercite el derecho del art. 6.2.b) LAECSP conserven la documentación acreditativa del efectivo ejercicio del mismo incorporándola al expediente en que el mismo se ejerció no se encontraba en la LAECSP pero puede ser añadida por el Reglamento de desarrollo de la LAECSP. Esto no entra en contradicción con la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de julio de 2010, que ha recordado la libertad de forma que tiene el responsable de fichero para la acreditación del cumplimiento del deber de información ya que no nos encontramos en este caso con un eventual responsable de fichero privado –que es titular del derecho y tiene las obligaciones establecidas por Ley– sino ante una Administración.

(155) El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio reitera en el art. 48 –«Imágenes electrónicas aportadas por los ciudadanos» que «la aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos»–.

(156) Lo mismo puede decirse de lo previsto en el art. 30.5 LAECSP que señala que las copias realizadas en papel de documentos públicos emitidos por medios electrónicos y firmados electrónicamente tienen la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otro sistema de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública emisora.

un certificado de otra o de que la Administración solicite el cotejo de una copia digitalizada aportada por el ciudadano. Se trata de admitir que la incorporación de datos personales en una solicitud implica la autorización a la Administración para que lleve a cabo una comprobación de esta información en otras bases de datos públicas. El Reglamento de desarrollo de la LOPD en su art. 11 –«Verificación de datos en solicitudes formuladas a las Administraciones Públicas»– señalaba que «[c]uando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la autenticidad de los datos». Lógicamente, la comprobación implica una revelación de datos ya que si bien hay supuestos donde esta comprobación da resultados positivos –se comprueba que el dato personal que aporta el ciudadano es cierto–, la sola posibilidad de que la comprobación ofrezca un resultado negativo –que la información aportada por el ciudadano no sea cierta, por ejemplo, que no se esté al día de las obligaciones tributarias o con la seguridad social– supone una comunicación de datos personales. Como es sabido, no le corresponde a una norma de rango reglamentario limitar un derecho fundamental, algo sometido a reserva de Ley, por lo que parece razonable la anulación del art. 11 del Reglamento por la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo –Sección Sexta–, de 15 de julio de 2010, por suponer «un tratamiento o cesión de datos sin consentimiento y sin la habilitación legal exigida por los artículos 6 y 11 de la Ley Orgánica»(157). Pues bien, a nuestro juicio, la formulación de solicitudes a la Administración en las que el interesado declare datos personales que obran en otros ficheros públicos podría suponer un consentimiento tácito para que la Administración lleve a cabo las comprobaciones necesarias sobre la autenticidad de los datos –y, por tanto, respetaría el art. 11.1 LOPD– siempre y cuando se informe a los interesados previamente y expresamente de esta comprobación y de todos los extremos contenidos en el art. 5 de la LOPD y siempre que esta comprobación sólo tenga efectos en el procedimiento administrativo para el que se realiza la solicitud –no suponga un consentimiento general para el futuro–, teniendo siempre el interesado la posibilidad de retirar su solicitud(158). Como hemos señalado antes, el consentimiento del intere-

(157) El recurrente sostenía que el precepto reglamentario era contrario a los arts. 6.2, 11.2.a) y 21 de la LOPD y a los arts. 6.2.b) y 9 de la LAECSP, al establecer un nuevo supuesto de tratamiento y cesión de datos por parte de las Administraciones Públicas sin consentimiento de los interesados, sin más habilitación que una norma reglamentaria.

(158) Como señala la Sentencia del Tribunal Supremo, de 15 de julio de 2010, el art. 11 del Reglamento fue introducido en atención a las observaciones que al proyecto de Reglamento formuló el Ministerio de Administraciones Públicas. No obstante, la propuesta de este Ministerio, a diferencia del texto finalmente aprobado, sí contenía una clara expresión de la existencia de un consentimiento tácito, algo semejante a lo que recoge el Real Decreto 1671/2009, de 6 de noviembre, antes analizado a propuesta también del Ministerio de Administraciones Públicas. Así, la redacción propuesta era: «La formulación por medios electrónicos

sado no tiene necesariamente que ser expreso sino que vale toda manifestación de voluntad libre, inequívoca, específica e informada –art. 3.h) LOPD–(159), sin perjuicio de las reglas específicas del consentimiento aplicables a los datos especialmente protegidos –art. 7–. Si una persona presenta una solicitud a la Administración afirmando datos personales que están en posesión de esta o de otra Administración Pública y se le informa previamente de que va a producirse una comprobación –automatizada o no– de esta información en otras bases de datos públicas, está dando su consentimiento para la comunicación de datos personales entre Administraciones Públicas, lógicamente sólo de estos datos y no de otros y sólo para este procedimiento. La clave del consentimiento tácito vuelve estar en el cumplimento del principio de información previa, expresa, precisa e inequívoca de la cesión y del resto de garantías que anteriormente hemos expuesto recogidas en el art. 5 LOPD. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero «cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar» –art. 11.3 LOPD–(160). Co-

---

de solicitudes en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas conllevará la autorización al órgano destinatario de la solicitud para que verifique la autenticidad de tales datos». Señala la Sentencia que «[l]a circunstancia de que en la redacción del precepto se hubiera omitido la implícita referencia que en el texto propuesto por el Ministerio de Administraciones Públicas se hacía a un consentimiento tácito, no permite inferir, contrariamente a lo que sostiene el Abogado del Estado, que el artículo 11 del Reglamento se acomoda a los artículos 6 y 11 de la Ley Orgánica cuando prescinde de la habilitación legal».

(159) En otro momento hemos afirmado que esta verificación de datos personales incluidos en las solicitudes formuladas a las Administraciones Públicas sería legítima en virtud del art. 11.2.c) de la LOPD que permite la comunicación de datos sin contar con el consentimiento del afectado en los supuestos en que «el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros» –art. 11.2.c) LOPD–. No obstante, si bien el art. 11.2.c) de la LOPD se aproxima en algún momento al consentimiento tácito, este precepto prevé cesiones a un tercero distinto de aquel con el que se mantiene la relación jurídica; en cambio, en el supuesto de la verificación de datos, la Administración con la que se mantiene la relación jurídica es la cesionaria de la información –no la cedente–.

(160) En esta misma dirección, el art. 12.2 del Reglamento de desarrollo de la LOPD señala que el afectado debe haber sido informado de la cesión de sus datos personales de «forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo». La Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de julio de 2010 ha confirmado la adecuación del art. 12.2 del Reglamento de desarrollo de la LOPD con el art. 11.2 de la LOPD –Fundamento Jurídico Séptimo–, señalando que tanto el precepto legal como el reglamentario, al exigir que la información comprenda la finalidad a la que se destinarán los datos y el tipo de actividad que desarrolla el cesionario, responden al concepto que del consentimiento ofrece el artículo 3.h) de la Ley, a saber: «toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan». Y conviene significarlo pues no se entiende que

rresponde al responsable «la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en el derecho» –art. 12.3 del Reglamento de desarrollo de la LOPD–.

La LAECSP se pronuncia sobre la verificación de datos entre Administraciones Públicas pero peligrosamente va más allá. Así, en un artículo que lleva por título «Iniciación de procedimientos por medios electrónicos», se señala que «[c]on objeto de facilitar y promover su uso, los sistemas normalizados de solicitud podrán incluir comprobaciones automáticas de la información aportada respecto de datos almacenados en sistemas propios o pertenecientes a otras administraciones e, incluso, ofrecer el formulario cumplimentado, en todo o en parte, con objeto de que el ciudadano verifique la información y, en su caso, la modifique y complete» –art. 35.3–. De esta forma, la comprobación automática de la información aportada respecto de datos almacenados en sistemas propios o pertenecientes a otras Administraciones dispondría de una previsión legal. Sin embargo, el precepto avanza más allá al ofrecer incluso «el formulario cumplimentado, en todo o en parte, con objeto de que el ciudadano verifique la información y, en su caso, la modifique y complete». Pues bien, el criterio sistemático de interpretación jurídica exige que esta previsión legal sea interpretada de conformidad con el art. 6.2.b) de la misma Ley, que establece que el derecho a no aportar datos y documentos que obren en poder de las Administraciones Públicas y las posibilidades que éstas tienen de recabar dicha información cuando se trate de datos personales requiere el consentimiento de los interesados o la existencia de una habilitación legal. Lógicamente este consentimiento puede ser manifestado de manera tácita, debiéndose cumplir todas las previsiones establecidas en el art. 2 del Real Decreto 1671/2009, de 6 de noviembre, especialmente que los interesados sean informados expresamente y *previamente* de que el ejercicio del derecho a no aportar la documentación implica su consentimiento para que el órgano administrativo recabe la información de otras Administraciones Públicas –además de que el consentimiento lo sea para un procedimiento concreto, que los interesados lo puedan revocar en cualquier momento y que se deje constancia acreditada del ejercicio del derecho del art. 6.2.b) LAECSP–. Difícilmente un formulario *previamente cumplimentado* por la Administración respeta el principio de información también *previa*, expresa, precisa e inequívoca de la comunicación de datos, de manera que se pueda manifestar un consentimiento tácito(161). Por ello, sólo es legítima esta com-

---

pueda darse cumplimiento al último precepto legal citado, fundamental en el ámbito de la protección de datos, si en la información facilitada para la autorización por el interesado de la cesión de sus datos no se expresa qué finalidad tiene la comunicación de los mismos y qué tipo de actividad desarrolla aquel a quien se le comunican.

(161) Hay que recordar que el principio de información forma parte del contenido esencial del derecho fundamental a la protección de datos personales y el Tribunal Constitucional ha interpretado en la Sentencia 292/2000, de 30 de noviembre de manera restrictiva los límites a este derecho del interesado, también de aquellos que puedan provenir de una norma con rango de Ley.

probación automatizada si es el propio interesado el que tiene derecho a ejercer esta comprobación, de manera que si detecta algún error, pueda corregir éste a través de medios electrónicos en su propia solicitud. No se trataría de la «verificación de datos en solicitudes formuladas a las Administraciones Públicas» establecida en el art. 11 del Reglamento –que habilita al órgano destinatario de la solicitud en el ejercicio de sus competencias para llevar a cabo las verificaciones necesarias para comprobar la autenticidad de los datos en las solicitudes que los ciudadanos formulen a la Administración– sino de una verificación que el propio interesado lleva a cabo sobre su información en manos de las Administraciones Públicas ya que no es legítima una verificación de la información por parte de éstas en virtud del art. 6.2.b) LAECSP si no es con el consentimiento del interesado, lo que requiere siempre la información previa, expresa, precisa e inequívoca para que, en su caso, pueda entenderse que se ha manifestado este consentimiento de manera tácita.

Hay que insistir que el art. 6.2.b) LAECSP reconoce un derecho del ciudadano a no aportar datos o documentos administrativos que obren en poder de las Administraciones Públicas, lo que supone el establecimiento de una obligación de la Administración de utilizar los medios electrónicos para recabar por sí misma esta información. De ninguna manera se impone al ciudadano una obligación, sobre todo considerando que se trata de procedimientos iniciados a petición del éste. La comunicación de datos entre Administraciones Públicas requiere la información previa y el consentimiento, al menos tácito, del interesado. En este marco, la lógica de los tres primeros supuestos –no del cuarto– antes analizados sería sustancialmente la misma. Así, por ejemplo, no es muy diferente autorizar a la Administración a que solicite a otra un certificado de empadronamiento a que yo aporte un dato de empadronamiento y la Administración verifique la autenticidad de ese dato. Si para la tramitación de un procedimiento administrativo hace falta un certificado de otra Administración Pública, sólo me cabe aportarlo o autorizar a la Administración para que lo obtenga. El hecho de que un ciudadano ejercite el derecho a no aportar datos y documentos que obren en poder de las Administraciones Públicas supone un consentimiento para la cesión, siempre que se le haya informado previamente. Si lo que aporto es una copia digitalizada de un documento debo admitir que la Administración lleve a cabo una comprobación –automatizada o no– del mismo en bases de datos de otras Administraciones Públicas, siempre que se me haya informado previamente. Por último, si afirmo datos personales en una solicitud ante la Administración y si se me informa que la inclusión de esta información supone asumir que la Administración verifique esta información en otras bases de datos públicas, estoy dando el consentimiento tácito para esta comunicación. Es importante que el responsable pueda acreditar siempre el cumplimiento del deber de información –de cualquiera de las formas admisibles en derecho– y de que el ciudadano ha ejercido el derecho previsto en el art. 6.2.b) de la LAECSP ya que es prueba del consenti-

miento tácito. Lógicamente siempre es más garantista que el consentimiento fuera expreso y no tácito, aunque este último cabe dentro de la LOPD(162). Por ello, es aconsejable recomendar que en los formularios donde se ofrece al ciudadano la posibilidad de no aportar datos y documentos que obren en poder de la Administración Pública se solicite el consentimiento expreso para que las Administraciones Públicas recaben esta información de manera electrónica, después de haber cumplido el principio de información del art. 5 de la LOPD(163).

3. OTROS SUPUESTOS QUE LEGITIMAN LA COMUNICACIÓN DE DATOS PERSONALES ENTRE ADMINISTRACIONES PÚBLICAS

La LOPD establece en los arts. 11.2 y 21 distintas posibilidades de comunicación de datos entre Administraciones Públicas aunque no exista el consentimiento del interesado. La principal, como hemos señalado antes, es que esta comunicación esté prevista en una Ley –art. 11.2.a) LOPD–(164). Esta comunicación sin consentimiento se produce en muchas ocasiones en procedimientos que no han sido iniciados voluntariamente por el interesado. Por eso, puede llamar la atención que la LAECSP reconozca que una norma con rango de ley puede exceptuar el consentimiento del interesado cuando éste ejerce el derecho a no aportar los datos y documentos que obren en poder de las Administraciones Públicas –art. 6.2.b) de la LAECSP– ya que las habilitaciones legales para la comunicación de datos personales sin consentimiento afectan principalmente a procedimientos que no han sido iniciados por los ciudadanos. Son muchos los supuestos legales que prevén la comunicación de datos personales entre Administraciones Públicas sin consentimiento del inte-

(162) No hay que olvidar, como más adelante señalaremos, que la Administración electrónica tiene que respetar la regulación específica del consentimiento para los datos especialmente protegidos –art. 7 LOPD–.

(163) Así, como hemos señalado anteriormente, los Reales Decretos 522/2006 y 523/2006, de 28 de abril, por los que se suprime la aportación de fotocopias del Documento Nacional de Identidad y del certificado de empadronamiento por parte de los interesados en los procedimientos administrativos tramitados por la Administración General del Estado requieren el consentimiento del interesado para que estos datos puedan ser consultados y comprobados por medios electrónicos por la propia Administración Pública, debiendo constar dicho consentimiento en la solicitud de iniciación del procedimiento o en cualquier otra comunicación posterior.

(164) Así, la publicación de datos personales por medios electrónicos –en un diario oficial o en una web institucional en abierto en Internet– como los resultados de los procedimientos de concurrencia competitiva, las sesiones o acuerdos de Plenos municipales o los listados de miembros de grupos profesionales, que significa no una comunicación de datos entre Administraciones Públicas sino de éstas a los ciudadanos, requiere una clara habilitación legal, sin perjuicio de la necesidad de respetar el principio de calidad. Ésta es una cuestión que hemos analizado en otro momento. Cfr. nuestro trabajo «Transparencia administrativa y protección de datos personales», en A. TRONCOSO REIGADA, *Transparencia administrativa y protección de datos personales*, Civitas-APDCM, Madrid, 2008, pp. 23-188.

resado que deberían materializarse a través de medios electrónicos. La LAECSP también circunscribe las comprobaciones automatizadas de datos entre Administraciones Públicas a la iniciación del procedimiento por parte del interesado –art. 35–. Asimismo regula la transmisión de datos entre Administraciones Públicas por medios electrónicos en relación al ejercicio del derecho de los ciudadanos a no aportar datos y documentos que obren en poder de la Administración –art. 9 LAECSP–. Esto es lógico ya que se trata de una Ley que regula el acceso electrónico de los ciudadanos a los servicios públicos y no de una Ley de Administración Electrónica. No obstante, hay que insistir en la importancia de la implantación de medios electrónicos en la transmisión de datos entre Administraciones Públicas en procedimientos no iniciados por los ciudadanos y en supuestos distintos al ejercicio por parte del ciudadano del derecho a no aportar datos y documentos que obren en poder de las Administraciones Públicas(165). La comunicación de datos personales entre Administraciones Públicas –entre órganos de la Administración General del Estado y de las demás Administraciones Públicas territoriales, entre éstas y las Administraciones Institucionales como la Agencia Estatal de Administración Tributaria o las entidades gestoras de la Seguridad Social, etc.– se debe hacer preferentemente por medios electrónicos. Como hemos señalado en otra ocasión, para que la comunicación de datos personales entre Administraciones Públicas sea legítima no es necesario que una Ley autorice expresamente la cesión sino que también puede reputarse como tal si se hace en virtud de competencias administrativas o para el cumplimiento de un deber que se encuentren regulados en normas con rango de ley(166).

---

(165) El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, establece que los órganos de la Administración General del Estado y sus organismos públicos deberán utilizar medios electrónicos para comunicarse entre ellos –art. 34–.

(166) La Administración Pública desarrolla una actividad administrativa en cumplimento de la vertiente prestacional de los derechos fundamentales y que requiere el tratamiento de datos personales. El principio de competencia puede ser en ocasiones un límite al derecho fundamental a la protección de datos personales si ésta encuentra acomodo en una norma con rango de Ley. Cfr. J. M. RODRÍGUEZ DE SANTIAGO, *La ponderación de bienes e intereses en el Derecho administrativo*, Marcial Pons, Madrid, 2000. Esta cuestión la hemos analizado en «La comunicación de datos personales», en A. TRONCOSO REIGADA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Cizur Menor, 2010, pp. 964-978. Sin embargo, la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de julio de 2010 –Sección Sexta– señala en relación con la anulación del art. 11 del Reglamento de desarrollo de la LOPD, que no debe tenerse en cuenta la aseveración de la Abogacía del Estado que justificaba «la potestad de verificación de la Administración cuando se encuentre en el ejercicio de sus competencias, pues una cosa es que ese ámbito competencial se encuentre amparado legalmente, consideración ésta aducida por el Abogado del Estado, y otra muy distinta que ese amparo legal no comprenda la habilitación legal específica exigida por la Ley Orgánica». No podemos estar de acuerdo con esta última aseveración de la Sentencia por las razones ya expuestas en otros trabajos de que debe entenderse como suficiente la existencia de una previsión legal que establezca las competencias administrativas que requieren el acceso a datos personales. Ni la Directiva 95/46/CE exige la necesidad de una Ley ni el resto de países de la Unión Europea exigen para la cesión de datos entre Adminis-

De manera específica, la LOPD regula las comunicaciones de datos entre Administraciones Públicas en el art. 21 –que se titula «Comunicación de datos entre Administraciones Públicas»–. Así, establece que «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 tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos» (art. 21.1 LOPD), lo que permite la comunicación de datos personales entre Administraciones Públicas distintas sin el consentimiento del interesado para el ejercicio de las mismas competencias o de competencias sobre las mismas materias. Después de un progresivo período de descentralización las Administraciones Públicas desarrollan en muchas ocasiones «competencias idénticas o que versan sobre las mismas materias» –art. 10.4.c) del Reglamento de desarrollo de la LOPD–, lo que requiere una comunicación de datos personales que debe hacerse por medios electrónicos para garantizar los derechos de los ciudadanos a la prestación de unos servicios públicos de calidad(167). Inicialmente la LOPD así como la LORTAD permitían la comunicación de datos entre Administraciones Públicas para el ejercicio de competencias diferentes o de competencias sobre materias distintas, cuando esta comunicación hubiera sido prevista por la disposición de creación de fichero o por disposición de superior rango que regule su uso. Esta previsión legal fue declarada inconstitucional a partir de la STC 292/2000, de 30 de noviembre, de forma que sólo es legítima la comuni-

---

traciones Públicas que la ley contemple expresamente la cesión. Esto sería lo ideal pero ya hemos comentado que son pocos los legisladores que están pensando en las cesiones de datos personales en el procedimiento legislativo. Sí es recomendable, como hemos señalado antes, que la Administración recabe el consentimiento expreso para las comunicaciones de datos personales en virtud del ejercicio del derecho establecido en el art. 6.2.b) de la LAECSP. Pero difícilmente puede bloquearse la actividad administrativa exigiendo que la Ley prevea la cesión expresamente, cuando el ejercicio de una competencia administrativa prevista en una Ley implique el acceso a información personal de la que disponga otra Administración –con el límite, que hemos señalado en otro momento, de que esta información no haya sido aportada voluntariamente por el interesado para una finalidad específica–. Esta situación no siempre es conocida por los Tribunales sino por las autoridades de control, especialmente por las Agencias Autonómicas de Protección de Datos cuya única competencia se circunscribe a las Administraciones Públicas y que desarrollan una actividad preventiva o de *prior checking*, informando la adecuación a la LOPD de innumerables solicitudes de cesiones de datos entre Administraciones Públicas. Esto demuestra que administrar y juzgar siguen siendo dos funciones distintas y complementarias, especialmente cuando la función de administrar recae en Administraciones Independientes que disponen de un conocimiento especializado sobre algunas materias. Cfr. L. PAREJO ALFONSO, *Administrar y juzgar: dos funciones constitucionales distintas y complementarias*, Tecnos, Madrid, 1993; y T. R. FERNÁNDEZ, *De la arbitrariedad de la Administración*, Civitas, Madrid, 1994.

(167) Éste sería el caso, por ejemplo, de la comunicación administrativa de datos personales entre servicios de salud o entre servicios sociales que gestionan las prestaciones de dependencia y que debe hacerse por medios electrónicos.

cación de datos entre Administraciones Públicas sin el consentimiento del interesado cuando sea para el ejercicio de competencias semejantes o de competencias sobre las mismas materias(168). La comunicación de datos entre Administraciones Públicas para funciones o materias distintas exige una habilitación legal o el consentimiento del interesado. Por tanto, no basta con que técnicamente sea posible la comunicación de datos entre distintas Administraciones Públicas por medios electrónicos, es necesario que sea jurídicamente legítimo(169). Las comunicaciones de datos entre Administraciones Públicas que se plantean frecuentemente son para el ejercicio de competencias distintas. De hecho, habitualmente sólo hay competencias comunes entre diferentes Administraciones territoriales (salud pública de un Ayuntamiento, salud pública de una CC AA y salud pública del Ministerio de Sanidad). La exigencia de que existan competencias administrativas comunes para que sea legítima la cesión de datos entre Administraciones Públicas equivale a requerir que las distintas bases de datos tengan finalidades compatibles. De esta forma, se puede afirmar que la comunicación de bases de datos entre Administraciones Públicas afecta esencialmente al principio de finalidad –que sea un tratamiento para la misma finalidad– o al principio de consentimiento –que se requiera el consentimiento cuando sea para una finalidad distinta, salvo que haya una habilitación legal–. No obstante, como hemos señalado anteriormente, la actuación de la Administración Pública sometida al principio de legalidad dentro de su reserva de Administración y en el ámbito de sus competencias puede ser suficiente para justificar una cesión de datos personales, siempre que se respeten otros principios y derechos de protección de datos, especialmente el de información. En todo caso, no es legítimo que un dato personal facilitado por el interesado por propia iniciativa para una finalidad sea empleado para finalidades distintas y por Administraciones distintas(170).

La LOPD prevé expresamente la comunicación de datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra –art. 21.2 LOPD–, una previsión que facilita la configuración de registros electrónicos comunes que permiten la comunicación de los datos desde el registro a la Administración destinataria que tenga la compe-

(168) Cfr. la crítica a esta Sentencia en nuestro trabajo «La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional», *Cuadernos de Derecho Público*, núms. 19-20, 2003, pp. 291-320.

(169) En este punto España tiene un régimen mucho más restrictivo para la Administración electrónica que el resto de países de la Unión Europea. La Directiva no diferencia la cesión del resto de los tratamientos y excluye la necesidad de contar con el consentimiento del interesado cuando el tratamiento sea «necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos» –art. 7.e)–. Cfr. nuestra «Introducción» a *An approach to data protection in Europe*, cit., pp. 14-23 y 26-33.

(170) Ésta es una cuestión sobre la que hemos profundizado en otro momento. Cfr. «La comunicación de datos personales», cit., pp. 979-997.

tencia para tramitar y resolver la solicitud(171). A estos efectos, la LAECSP lleva a cabo una regulación de los registros electrónicos que deroga las previsiones más restrictivas de la LRJAP y PAC(172). Así, la LAECSP crea registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones –art. 24.1–, donde se podrán admitir cualquier escrito dirigido a cualquier órgano o entidad del ámbito de la Administración titular del registro –art. 24.2–. Además establece que en cada Administración Pública existirá, al menos, «un sistema de registros electrónicos suficiente para recibir todo tipo de solicitudes, escritos y comunicaciones dirigidos a dicha Administración Pública –art. 24.3–. Las Administraciones Públicas podrán, mediante convenios de colaboración, habilitar a sus respectivos registros para la recepción de solicitudes, escritos y comunicaciones de la competencia de otra Administración que se determinen en el correspondiente convenio». La LAECSP obliga a la Administración General del Estado a automatizar las oficinas de registro del art. 38 de la LRJAP y PAC para «garantizar la interconexión de todas sus oficinas y posibilitar el acceso por medios electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados» –art. 24.2–. La LOPD también establece que no será preciso el consentimiento «cuando la cesión se produzca entre Administraciones Públicas y

(171) También se puede aplicar a este supuesto la previsión contenida en el art. 11.2.c) de la LOPD, que permite la cesión cuando responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique la conexión de dicho tratamiento con ficheros de terceros.

(172) La LAECSP deroga el art. 38.9 de la LRJ-PAC que establecía que «[s]e podrán crear registros telemáticos para la recepción o salida de solicitudes, escritos y comunicaciones que se transmitan por medios telemáticos, con sujeción a los requisitos establecidos en el apartado 3 de este artículo. Los registros telemáticos *sólo estarán habilitados para la recepción o salida de las solicitudes, escritos y comunicaciones relativas a los procedimientos y trámites de la competencia del órgano o entidad que creó el registro y que se especifiquen en la norma de creación de éste*, así como que cumplan con los criterios de disponibilidad, autenticidad, integridad, confidencialidad y conservación de la información que igualmente se señalen en la citada norma». Este precepto fue objeto de desarrollo por el Real Decreto 772/1999, de 7 de mayo, que regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro, modificado por el Real Decreto 209/2003, de 21 febrero. Sin embargo, hay que señalar que el art. 38.4 de la LRJ-PAC prevé, en su apartado b) que «las solicitudes, escritos y comunicaciones que los ciudadanos dirijan a los órganos de las Administraciones Públicas podrán presentarse (...) en los registros de cualquier órgano administrativo, que pertenezca a la Administración General del Estado, a la de cualquier Administración de las Comunidades Autónomas, o a la de alguna de las entidades que integran la Administración Local si, en este último caso, se hubiese suscrito el oportuno convenio. Mediante convenios de colaboración suscritos entre las Administraciones Públicas se establecerán sistemas de intercomunicación y coordinación de registros que garanticen su compatibilidad informática, así como la transmisión telemática de los asientos registrales y de las solicitudes, escritos, comunicaciones y documentos que se presenten en cualquiera de los registros». Hay que recordar que el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio ha derogado los arts. 14 al 18 del Real Decreto 772/1999, de 7 de mayo así como el Real Decreto 263/1996, de 16 de febrero.

tenga por objeto el tratamiento posterior con fines históricos, estadísticos o científicos» –arts. 11.2.e) y 21.1–, un supuesto de comunicación de datos personales entre Administraciones Públicas que debe impulsarse también por medios electrónicos.

La LOPD también prevé otras cesiones sin consentimiento del interesado y que también pueden realizarse por medios electrónicos. Así, la LOPD establece que el consentimiento no será necesario cuando la cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros [art. 11.2.c) LOPD] (173) o cuando la comunicación tenga por destinatario al Defensor del Pueblo, Ministerio Fiscal, Jueces o Tribunales o Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas, así como a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas [art. 11.2.d) LOPD] (174). También permite la excepción del consentimiento «cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica» [art. 11.2.f) LOPD]. Hay que recordar que no es legítima la comunicación de datos especialmente protegidos por medios electrónicos en virtud de un consentimiento tácito sino que es preciso aplicar las reglas de consentimiento establecidas de manera específica en el art. 7 de la LOPD. Así, la comunicación entre Administraciones Públicas de datos de salud por medios electrónicos exige el consentimiento expreso

(173) En muchos supuestos la existencia de un consentimiento tácito es muy próxima a la excepción del consentimiento del afectado cuando «el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros» –art. 11.2.c) LOPD–. Hemos afirmado antes que en la verificación de datos incluidos en solicitudes formuladas a las Administraciones Públicas existe un consentimiento tácito cuando se informa previamente al interesado de que va a producirse una comprobación automatizada de esta información en otras bases de datos públicas. Igualmente existe un consentimiento tácito cuando una orden de subvenciones afirma expresamente que los certificados no aportados por el interesado puedan ser solicitados de oficio por la propia Administración. La clave para aplicar a estos dos supuestos la excepción del consentimiento prevista en el art. 11.2.c) LOPD es entender que la aceptación de una relación jurídica y de todo aquello que sea necesario para su desarrollo, cumplimiento y control no sólo permite cesiones de información a un tercero distinto de aquel con el que se mantiene la relación jurídica sino también ser cesionarios de información procedente de terceros, entendiendo que el art. 11.2.c) no habla de cesiones sino de la conexión de dicho tratamiento con ficheros de terceros.

(174) La aplicación de medios electrónicos a la cesión de datos recogidos de fuentes accesibles al público –art. 11.2.b)– se encuentra limitada por la prohibición de comunicar estos datos a ficheros de titularidad privada salvo que exista consentimiento del interesado o una Ley que así lo prevea –art. 21.3 LOPD–.

o la habilitación legal –arts. 7.3 y 11.2.a) LOPD–(175). Ya hemos analizado en otro momento las implicaciones que suponen la historia clínica electrónica y la receta electrónica(176). En todo caso, la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud, así como la legislación autonómica permiten la comunicación de datos de salud por medios electrónicos entre los centros sanitarios públicos y privados dentro del Sistema Nacional de Salud(177).

4. LOS ACCESOS AUTOMATIZADOS, LAS INTERCONEXIONES DE BASES DE DATOS Y EL RESPETO A LOS PRINCIPIOS DE CALIDAD Y DE PROPORCIONALIDAD

La comunicación de datos personales, especialmente si se hace en virtud de una habilitación legal –pero también si se hace con el consentimiento del interesado–, tiene que ser respetuosa con el principio de calidad y de finalidad. Este principio, que es de aplicación a todos los tratamientos de datos personales y también a las comunicaciones de datos personales desde ficheros no automatizados, tiene una especial relevancia en el ámbito de la Administración electrónica. La LAECSP afirma en la Exposición de Motivos –como ya se ha citado anteriormente– que «la progresiva utilización de medios electrónicos suscita la cuestión de la privacidad de unos datos que se facilitan en relación con un expediente concreto pero que, archivados de forma electrónica como consecuencia de su propio modo de transmisión, hacen emerger el problema de su uso no en el mismo expediente en el que es evidente, desde luego, pero, sí la eventualidad de su uso por otros servicios o dependencias de la Administración o de cualquier Administración o en otro expediente. Las normas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección

(175) La comunicación por medios electrónicos de datos especialmente protegidos requiere una clara habilitación legal, como la que suministra la Disposición Adicional Primera de la Ley 27/2003 de Reforma de la Ley de Enjuiciamiento Criminal y la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, que ha posibilitado la organización del Registro Central para la Protección de las Víctimas de la Violencia Doméstica, que permite que Fuerzas y Cuerpos de Seguridad, Juzgados de Violencia sobre la Mujer, servicios sanitarios y servicios sociales accedan a datos personales para la prevención, asistencia y persecución de los actos de violencia de género, etc. La comunicación de datos especialmente protegidos la hemos analizado en «La comunicación de datos personales», cit., pp. 997-1006.

(176) La comunicación de las historias clínicas dentro del Sistema Nacional de Salud y la receta electrónica la hemos abordado en «Introducción y Presentación» a *Protección de datos personales para Servicios Sanitarios Públicos*, Civitas-APDCM, Madrid, 2008, pp. 115-136.

(177) El Reglamento de desarrollo de la LOPD establece que, «en particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud» –art. 10.5–.

de DCP deben bastar, y no se trata de hacer ninguna innovación al respecto, pero sí de establecer previsiones que garanticen la utilización de los datos obtenidos de las comunicaciones electrónicas para el fin preciso para el que han sido remitidos a la Administración» –apdo. III–. La propia LAECSP reitera que «[p]ara un eficaz ejercicio del derecho reconocido en el apartado 6.2.b), cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico […]. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. El acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b) de la presente Ley» –art. 9–. Por tanto, con anterioridad a la comunicación de datos es imprescindible analizar el respeto al principio de finalidad, valorando si los datos han sido facilitados voluntariamente por el interesado para un expediente concreto y, por tanto, para una finalidad concreta y específica y no pueden ser empleados para finalidades incompatibles con «el fin preciso para el que han sido remitidos a la Administración»(178), y si la finalidad es legítima y, por lo tanto, si entra dentro de la reserva de Administración –si los datos son requeridos a los ciudadanos por las Administraciones Públicas «para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos»–. La comunicación de datos sólo puede producirse entre Administraciones Públicas que actúan en el ámbito de sus competencias –sólo así puede entenderse que una Administración Pública actúa legítimamente–, lo que habilita para comprobar si la Administración cesionaria tiene la competencia administrativa para reclamar la información. Además, hay que analizar específicamente el principio de calidad como principio de adecuación y prohibición de exceso de forma que los datos requeridos tienen que estar previstos en la normativa administrativa, debiendo limitarse la comunicación «a aquellos datos que son requeridos a los ciudadanos por las restantes Administraciones». Lógicamente, los datos deben ser cancelados por la Administración cesionaria cuando se haya cumplido la finalidad para la cual han sido recabados –art. 4.5 LOPD–.

La Administración electrónica no sólo permite las cesiones de datos entre Administraciones Públicas sino también el acceso automatizado y

(178) Es muy importante que las comunicaciones de datos personales por medios electrónicos respeten el principio de finalidad, especialmente cuando se trata de información personal aportada voluntariamente por el interesado para una finalidad concreta –para obtener una prestación social o una ayuda– y donde no se empleó la excepción del consentimiento para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, como ocurre en el caso de las funciones públicas de soberanía –art. 6.2 LOPD–.

la interconexión permanente de bases de datos de las Administraciones Públicas(179). Así, la LAECSP establece que la Administración General del Estado y las Administraciones Autonómicas, así como las entidades que integran la Administración local que lo soliciten, posibilitarán «la interconexión de sus redes con el fin de crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas españolas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros» –art. 43–(180). Ya hemos mencionado antes cómo la LAECSP establece un «principio de cooperación en la utilización de medios electrónicos por las Administraciones Públicas al objeto de garantizar tanto la interoperabilidad de los sistemas y soluciones adoptados por cada una de ellas como, en su caso, la prestación conjunta de servicios a los ciudadanos» –art. 4.e)–. Ha señalado así COTINO HUESO que parecemos «abocados al modelo de Administración electrónica de intercambiabilidad total de datos sin intervención directa de órganos ni personal administrativo en los procesos de comunicación»(181). En todo caso, hay que tener en cuenta que no es lo mismo la cesión de datos personales, el acceso automatizado y la interconexión entre bases de datos ya que los últimos dos supuestos –especialmente el tercero– incrementan el riesgo y suponen una mayor injerencia en el derecho fundamental a la protección de datos. En la cesión de datos personales el responsable del fichero puede desarrollar una comprobación individualizada de que la comunicación solicitada cumple la legislación de protección de datos y, especialmente, las causas de legitimación para la cesión –que existe el consentimiento del interesado aunque sea

(179) Cfr. J. VALERO TORRIJOS, «El acceso telemático a la información administrativa: un presupuesto inexcusable para la e-Administración», en L. COTINO HUESO (Coord.), *Libertades, democracia y gobierno electrónicos*, Comares, Granada, 2006, pp. 199-227. Cfr. Documento de trabajo del Grupo de Protección de datos del art. 29, relativo a la Administración en línea, *cit.* Sobre las infraestructuras de la interoperabilidad, en concreto sobre la red de comunicaciones de las Administraciones Públicas como la Red SARA –Sistema de Aplicaciones y Redes para las Administraciones– que es una red privada creada en 2006 que permite la interconexión a todos los Ministerios de la Administración General del Estado, a las Comunidades Autónomas y que está conectada con la Unión Europea, o sobre la Red 060 de atención al ciudadano multicanal y multi-administraciones, creada en 2005 –*www.csae.map.es*–, cfr. A. CERRILLO, «La interoperabilidad y la protección de datos», cit., pp. 49-50. En Italia, está en ejecución un proyecto nacional de creación de una «red de la Administración Pública unificada», esto es, una red electrónica que conectará a todas las autoridades administrativas del país.

(180) Hay que tener en cuenta, además, que las comunicaciones de datos dirigidas a Administraciones Públicas Europeas tienen el carácter de transferencia internacional de datos y deben seguir su específico régimen jurídico –arts. 33-34 LOPD–.

(181) Cfr. L. COTINO HUESO, «Derechos del ciudadano», cit., p. 196, siguiendo la posición de J. VALERO TORRIJOS, «Acceso a los servicios y difusión de la información por medios electrónicos», p. 269, que resalta que «la principal singularidad que plantea esta nueva modalidad de comunicación administrativa es su automatización». Ambos trabajos están en E. GAMERO CASADO y J. VALERO TORRIJOS (Coord.), *La Ley de Administración Electrónica,* cit.

tácito, previo cumplimiento del principio de información, una habilitación legal, una relación negocial o que la cesión sea para competencias semejantes sobre materias comunes– y del principio de calidad. Por tanto, la solicitud de cesión concreta facilita la acreditación de estos extremos ante el cedente y eventualmente ante la propia autoridad de control(182). También permite la información al ciudadano cuando éste ejercite su derecho de acceso del art. 15 de la LOPD que implica conocer las concretas cesiones de sus datos que se han realizado a otras Administraciones. En cambio, en el acceso automatizado y en las interconexiones, la Administración cedente se limita a poner la información personal a disposición del cesionario, desapareciendo la supervisión administrativa por parte del cedente del cumplimiento en cada caso de los requisitos legales y que sólo puede implementarse si esta evaluación es desarrollada *ex ante* y si los sistemas de información permiten una comprobación automatizada del cumplimiento de los requisitos legales para la comunicación que garanticen el respeto al derecho fundamental a la protección de datos personales. Lógicamente, todo esto es aún más complejo en el caso de las interconexiones de bases de datos donde en muchas ocasiones desaparece el rastro, impidiendo que el interesado conozca al ejercitar el derecho de acceso quiénes han sido los cesionarios de la información. En cambio, el acceso automatizado al menos deja constancia del usuario que llevó a cabo el acceso, de la fecha y hora, de los datos consultados(183) e, incluso, posibilita algún control automatizado en cada su-

(182) Ya hemos señalado antes que el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, ha regulado las transmisiones de certificados, datos y documentos entre organismos de la Administración General del Estado, estableciendo que los órganos u organismos ante los que se ejercite el derecho a no aportar datos y documentos que obren en poder de las Administraciones Públicas conservarán la documentación acreditativa del efectivo ejercicio del derecho incorporándola al expediente en que el mismo se ejerció, estando a disposición del órgano cedente y de las autoridades a las que en su caso corresponda la supervisión y control de la legalidad de las cesiones producidas –art. 2–.

(183) La Ley Orgánica 14/2003, ha incorporado una nueva disposición adicional séptima a la LBRL titulada «Acceso a los datos del Padrón» donde se afirma que «[p]ara la exclusiva finalidad del ejercicio de las competencias establecidas en la Ley Orgánica de Derechos y Libertades de los Extranjeros en España y su Integración Social, sobre control y permanencia de extranjeros en España, la Dirección General de la Policía accederá a los datos de inscripción padronal de los extranjeros existentes en los padrones municipales, preferentemente por vía telemática. A fin de asegurar el estricto cumplimiento de la legislación de protección de datos de carácter personal, los accesos se realizarán con las máximas medidas de seguridad. A estos efectos, quedará constancia en la Dirección General de la Policía de cada acceso, la identificación de usuario, fecha y hora en que se realizó, así como de los datos consultados». No se establece una solicitud de acceso al Padrón Municipal dirigida al Ayuntamiento –que tendría que ser autorizada por éste– ya que la propia Dirección General de la Policía tendrá acceso directo al padrón municipal para la exclusiva finalidad del control de la inmigración irregular. Si bien no habrá petición escrita, el sistema de información deberá dejar la identificación de usuario, fecha y hora en que se realizó el acceso, así como de los datos consultados. Esto obligará al fichero del Padrón Municipal a disponer de unas medidas de seguridad de nivel alto. La misma Ley incorpora también

puesto concreto(184). Todo esto obliga a que tanto el responsable del fichero como los eventuales cesionarios definan un modelo de intercambio de información que se adecue a la legislación de protección de datos, teniendo en cuenta que un eventual incumplimiento supone la aplicación de un riguroso régimen sancionador sobre todo para el responsable del fichero y cedente pero que también puede alcanzar al cesionario. Así, si se establece un modelo de accesos automatizados y de interconexiones, es necesario determinar previamente cuál es la legitimación que justifica la cesión de datos personales –si existe una habilitación legal o consentimiento del interesado y cuál es el procedimiento para dejar constancia de este último–. A nuestro juicio, las Administraciones Públicas tienen que optar por el consentimiento expreso para la interoperabilidad. También es necesario garantizar el cumplimiento del principio de calidad y de finalidad –que sólo se accede a datos adecuados y no excesivos para el ejercicio de competencias administrativas por parte del órgano cesionario y, por tanto, no a toda la información personal que sobre esa persona dispone el cedente que es para sus propias competencias administrativas–. Es preciso determinar también quiénes son los usuarios autorizados por parte del órgano cesionario para acceder a la información(185). Los accesos automatizados y las interconexiones tienen que respetar el principio de seguridad, por ejemplo, el cifrado cuando se trate de datos especialmente protegidos, policiales o de violencia de género y se utilicen

---

una Disposición Adicional Quinta en la Ley Orgánica 4/2000, de 11 de enero, por la que se regula los Derechos y Libertades de los Extranjeros en España y su Integración Social: «En el cumplimiento de los fines que tienen encomendadas, y con pleno respeto a la legalidad vigente, las Administraciones Públicas, dentro de su ámbito competencial, colaborarán en la cesión de datos relativos a las personas que sean consideradas interesados en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo. Para la exclusiva finalidad de cumplimentar las actuaciones que los órganos de la Administración General del Estado competentes en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo tienen encomendadas, la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social *y el Instituto Nacional de Estadística, este último en lo relativo al Padrón Municipal de Habitantes*, facilitarán a aquéllos el acceso directo a los ficheros en los que obren datos que hayan de constar en dichos expedientes, y sin que sea preciso el consentimiento de los interesados, de acuerdo con la legislación sobre protección de datos». En este último caso no se prevén medidas de seguridad.

(184) Hemos analizado en otro momento cómo en los accesos automatizados a algunos registros públicos se ha tratado de respetar el principio de calidad y proporcionalidad, evitando que estos accesos se produzcan para finalidades incompatibles y estableciendo cautelas frente a la obtención masiva de datos personales y su utilización para finalidades comerciales. Cfr. nuestro trabajo «Transparencia administrativa y protección de datos personales», cit., pp. 135-141.

(185) Así, el art. 20 LAECSP relativo al intercambio electrónico de datos en entornos cerrados de comunicación señala que cuando los participantes en la comunicación pertenezcan a la misma Administración Pública, ésta establecerá las condiciones y garantías por las que se regirá, que comprenderá al menos la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar. Cuando los participantes pertenezcan a distintas Administraciones Públicas, estas condiciones y garantías se establecerán mediante convenio.

redes públicas de comunicaciones. Igualmente, es necesario informar al interesado de cuáles son las Administraciones Públicas que están interconectadas o que pueden acceder a la información y para qué finalidad y tipo de actividad. Además, es necesario garantizar el derecho del interesado a solicitar información sobre las comunicaciones realizadas, lo que obliga a establecer alguna trazabilidad de las interconexiones que permita que quede constancia «en los ficheros del órgano u organismo cedente del acceso a los datos o documentos efectuado por el órgano u organismo cesionario» –art. 2 del Real Decreto 1671/2009, de 6 de noviembre–. Como hemos señalado antes, la *privacy by design* ocupa aquí de nuevo un papel central para que sea el cumplimiento de concretas competencias administrativas y el respeto a la legislación de protección de datos lo que defina los flujos de datos personales entre Administraciones Públicas. Igualmente, el establecimiento de repositorios comunes de datos personales para facilitar el intercambio de información entre órganos de la misma o de distinta Administración Pública exige el respeto a los principios y derechos de protección de datos personales establecidos en la LOPD(186). Así, no pueden crearse ficheros de datos personales para

(186) La LAECSP obliga a todos los órganos administrativos que traten datos personales de los ciudadanos a facilitar esta información a otros órganos de la misma o de otras Administraciones Públicas en el ámbito de sus competencias. Para cumplir esta obligación las Administraciones Públicas pueden optar por facilitar esa información en cada supuesto o por crear repositorios comunes de datos y documentos personales para intercambiar información que deben estar disponibles en entornos cerrados de comunicaciones, no accesibles por terceros. Lógicamente, la puesta a disposición de información para otros órganos de la misma o de distinta Administración requiere del cumplimiento de las garantías legales. El acceso a esta información sólo puede ser realizado previa acreditación de la existencia de una habilitación legal, del consentimiento del interesado o de la necesidad de verificar la exactitud de datos facilitados por éste y que se encuentran en poder de las Administraciones Públicas, debiendo existir en este caso un consentimiento tácito, previo cumplimiento del principio de información. Asimismo, es necesario especificar la relación de emisores y receptores de información autorizados y la naturaleza de los datos a intercambiar. Por ello, es conveniente que la implantación de un repositorio de datos y/o documentos cuente con un informe emitido por la autoridad de protección de datos en quien resida la competencia sobre el tratamiento de los datos. Los sistemas de acceso a esos ficheros o repositorios deberán gestionarse mediante la realización de consultas individualizadas de datos concretos de personas determinadas, acreditando la identidad del solicitante de la información, su finalidad y la legitimación que habilita la petición que efectúa. En ningún caso debe facilitarse el acceso de forma masiva a cualquiera de los ficheros o repositorios destinados al intercambio de información entre órganos de la misma o distinta Administración Pública. Cfr. sobre esta cuestión la Recomendación 3/2008 de la APDCM sobre tratamiento de datos de carácter personal en los servicios de Administración electrónica.

Hay que resaltar el proyecto irlandés de Administración electrónica, del que se hace eco el documento de trabajo del Grupo del Artículo 29 ya citado. En este proyecto, la prestación de los servicios públicos se hace mediante un agente que «almacena en una cámara de seguridad los datos personales que se usen con frecuencia (por ejemplo, los relativos al nacimiento, el pasaporte, los ingresos, las relaciones familiares, etc.) y los gestionará y protegerá en beneficio del usuario. Los datos sólo se darán a conocer a una agencia de servicios públicos cuando el usuario dé instrucciones concretas, en caso de transacción, con motivo de un servi-

que sean compartidos por distintas Administraciones para finalidades también distintas e incompatibles, salvo que exista una clara habilitación legal(187).

Por ello, en el caso de comunicaciones de datos entre Administraciones Públicas para finalidades distintas es mejor optar por cesiones concretas o por un acceso automatizado que permita establecer puntos de control y no ir hacia un modelo de interconexión permanente de bases de datos, salvo en supuestos claros en que esté justificado. Específicamente, el establecimiento de un modelo de interconexión de bases de datos tiene que respetar el principio de proporcionalidad(188), especialmente de la proporcionalidad en sentido estricto, que exige que la medida adoptada –la injerencia en el derecho fundamental a la protección de datos personales– sea ponderada o equilibrada con el fin que se persigue, teniendo en cuenta la naturaleza del derecho lesionado, la intensidad de la injerencia y el bien o valor constitucional que se persigue. Esto obliga a llevar a cabo una valoración en cada caso sobre el equilibro entre el fin de la interconexión –el interés público y las potenciales ventajas para los ciudadanos en un procedimiento administrativo concreto– y la limitación que esto supone en el derecho fundamental a la protección de datos personales –especialmente en lo que hace referencia a la tipología de datos objeto de tratamiento–, teniendo en cuenta que las expectativas de los ciudadanos no sólo se extienden a la eficacia de los servicios públicos sino también a la protección de sus datos personales(189). También, es necesario llevar a cabo un juicio de necesidad que tenga en cuenta si existen otros medios posibles que permitan alcanzar ese interés público y la ventaja de los ciudadanos en el servicio administrativo concreto con

---

cio en el que intervenga el agente. Una vez desarrollado el sistema, el agente podrá prever ciertos sucesos (una pensión, por ejemplo) y cada categoría del sistema podrá sugerir cuestiones de interés para el individuo. Por medio del portal, el agente ofrecerá una «ventanilla única» a las personas que hagan uso de los servicios públicos. Paulatinamente, a medida que se sucedan las visitas, los servicios se podrán ir personalizando. La administración podrá garantizar que la vida privada del usuario se respeta, pues éste habrá dado su consentimiento para que sus datos se utilicen y almacenen de este modo con miras a la prestación del servicio de que se trate. La Autoridad irlandesa ha aprobado el uso de este modelo siempre y cuando se apliquen condiciones estrictas de protección de datos relativas al consentimiento y al uso de los datos para determinados fines».

(187) Así, por ejemplo, no es legítima la creación de una base de datos con información sobre víctimas de delitos con acceso a las Fuerzas y Cuerpos de Seguridad, Poder Judicial, Ministerio Fiscal y Servicios Sociales si no existe una ley que lo autorice, ya que se trata de cesiones para finalidades incompatibles.

(188) Cfr. M. MEDINA GUERRERO, «El principio de proporcionalidad», *Cuadernos de Derecho Público*, nº 5, 1998 y M. GONZÁLEZ BEILFUSS, *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional*, Aranzadi, Pamplona, 2003. Cfr. nuestra «Introducción» a *An approach to data protection in Europe*, cit., pp. 23-55.

(189) Cfr. sobre esta cuestión las referencias al Informe del Gobierno Británico «Privacy and data sharing: the way forward for public services», que se recoge en el Documento de Trabajo del Grupo del Artículo 29 ya citado, donde se señala que «las interconexiones no son indispensables para mejorar los servicios de la Administración».

un menor nivel de intromisión en el derecho fundamental a la protección de datos personales, ya que es necesario buscar siempre la medida más moderada para alcanzar la finalidad con la misma eficacia. Al igual que en el ámbito de la publicación de datos personales, se echa en falta una regulación más específica sobre las interconexiones de datos personales. Es necesario que las Autoridades de Protección de Datos informen preceptivamente las solicitudes de interconexión y que las Administraciones Públicas introduzcan todas las garantías posibles –por ejemplo, un sistema de comprobación automatizada de que se cumplen los requisitos legales y medidas de seguridad que minimicen los riesgos– que permitan un mayor equilibro entre el interés público y los límites al derecho a la protección de datos personales. Si bien no es posible establecer un sistema de autorizaciones de la Agencia de Protección de Datos para todas las comunicaciones de datos entre Administraciones Públicas, sí, al menos, debe exigirse al responsable administrativo que justifique la necesidad de introducir un modelo de interconexión de bases de datos y la autoridad de control debe valorar la solicitud a la luz del principio de calidad y de proporcionalidad a través de un informe preceptivo y vinculante(190).

No todos los accesos de terceras personas a un fichero tienen la

---

(190) Hasta ahora las interconexiones de los sistemas de información con la finalidad de garantizar el derecho de los ciudadanos a no aportar datos y documentos que ya obren en poder de las Administraciones se ha realizado sobre la base de la autorización expresa del interesado, lo que sin duda ha simplificado los trámites que ciudadanos y empresas deben realizar con las Administraciones Públicas, eliminando mucha documentación en papel. Tradicionalmente las Administraciones Públicas tienen Convenios con la Policía Nacional para consultar las bases de datos con la finalidad de verificar la identidad y obtener copias del DNI, con la Agencia Tributaria para consultar la situación de estar o no al corriente de pago y con el Instituto Nacional de Estadística para consultas relativas a la residencia. Especialmente la Tesorería General de la Seguridad Social ha firmado Convenios de Colaboración con las Comunidades Autónomas sobre intercambio recíproco por medios electrónicos de algunos datos de los ciudadanos. Así, es habitual que para la tramitación de sus expedientes la Consejería de Servicios Sociales requiera información relativa a las situaciones de alta en la Seguridad Social en determinada fecha o sobre situación de desempleo, que la Consejería de Empleo necesite llevar a cabo consultas relativas a la afiliación a la Seguridad Social y a las cuentas de cotización, que la Consejería de Sanidad lleve a cabo consultas sobre datos de asistencia sanitaria, modificación de zonas médicas, así como situaciones adicionales de afiliación a la seguridad social o que la Consejería de Economía necesite información de estar al corriente de pago en la seguridad social para un procedimiento de subvenciones. También la Consejería de Justicia necesita para la tramitación de los expedientes de justicia gratuita información de la Tesorería General de la Seguridad Social en relación con los días que el ciudadano ha permanecido en alta en la Seguridad Social. Recíprocamente la Tesorería General de la Seguridad Social para el cumplimiento de sus funciones administrativas requiere el acceso a información de las Comunidades Autónomas como los datos relativos a una demanda de empleo, certificados de título de familia numerosa, certificados de minusvalía, registro de inscripción de empresas en la Dirección General de Industria o certificados de estar al corriente de pago en la Administración Autonómica en los procedimientos de contratación y en los procedimientos de subvenciones.

consideración de cesión de datos personales. La LOPD señala que «no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento» –art. 12 LOPD–(191). Hay que recordar que si la Administración se apoya en empresas externas para desarrollar los servicios públicos electrónicos, es necesario que exista un contrato escrito por el cual la empresa se constituya en encargado del tratamiento y se obliga a lo establecido en el art. 12 de la LOPD(192). Esto ocurre en el caso de las autoridades de validación en lo relativo al DNI electrónico. Así, en este último caso, si bien las funciones de autoridad de registro –que toma los datos acreditativos de la identidad personal, fotografía, firma manuscrita y huella digital– y la autoridad de certificación –que expide los certificados electrónicos– es la Dirección General de la Policía, las autoridades de validación –que ofrecen al ciudadano servicios en los que reconoce el DNI electrónico y se comprueba la identidad y la vigencia de la firma– pueden ser tanto Entidades Públicas como privadas, siempre dentro del marco jurídico de encargados del tratamiento, por lo que deben cumplirse los requisitos establecidos en el art. 12 de la LOPD(193).

---

(191) La existencia de un encargado del tratamiento debe estar considerada expresamente en el procedimiento de contratación administrativa –Disposición Adicional Trigésimo Primera de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público–. El responsable del tratamiento está obligado a velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en la legislación de protección de datos personales –art. 20.2 del Reglamento–. El art. 21 del Reglamento de desarrollo de la LOPD regula las posibilidades de subcontratación.

(192) El documento de trabajo del Grupo del Artículo 29 también analiza la posibilidad de que los procedimientos administrativos en línea se encarguen a empresas privadas, una cuestión en la que no se obtuvo la misma respuesta en los diferentes países de la Unión. La Resolución de la APDCM, de 29 de julio de 2009, declaró una infracción grave prevista en el art. 44.3.d) de la LOPD al Ayuntamiento de Madrid por suscribir un contrato con una empresa para la prestación del servicio consistente en el «Suministro de equipos para la captura y emisión electrónica de denuncias de tráfico con destino al Departamento de Vigilancia de la Movilidad», en la que esta empresa accedía a datos personales constituyéndose en encargada del tratamiento sin incorporar el contrato las cláusulas del art. 12 de la LOPD.

La Ley 2/2011, de 4 de marzo, de Economía Sostenible en su Disposición final quincuagésima sexta ha modificado la LOPD en este punto. Así, la transmisión de datos a un encargado del tratamiento sin dar cumplimiento a los *deberes formales* establecidos en el art. 12 LOPD pasa a ser infracción leve –nuevo art. 44.2.d)–, cuando con anterioridad podía ser grave o muy grave –si se consideraba como una vulneración de los principios y garantías del antiguo 44.3.d) como en el ejemplo antes mencionado o si se calificaba como cesión de datos del art. 44.4.a)–. Otros incumplimientos que no sean deberes formales, como es el caso de las medidas de seguridad, tendrían otra calificación –por ejemplo, el de las medidas de seguridad será infracción grave en el nuevo art. 44.3.h)–.

(193) El documento del Grupo del Artículo 29 ya citado señala que la mayor parte de las delegaciones indican que en sus respectivos países está o estaría permitida la participación de operadores privados, «proveedores de servicios de certificación», en el marco de la aplicación de los mecanismos de firma electrónica en ciertos procedimientos administrativos en línea. En estos casos, el estatuto del proveedor de servicios de certificación está dotado de un

Como hemos señalado anteriormente, también puede acudirse a la figura del encargado del tratamiento cumpliendo lo establecido en el art. 12 de la LOPD a los efectos de alojar el sitio web de las Administraciones Públicas en servidores de terceros –ya sean entidades privadas u otras personas jurídicas públicas–(194). A nuestro juicio no existen cesiones dentro del marco de una misma persona jurídica pública –la Administración General del Estado, la Administración Autonómica o el Ayuntamiento correspondiente– por lo que la utilización de los servidores de otros Departamentos dentro de la misma persona jurídica pública no sería una cesión –no habría que firmar un convenio de encargo del tratamiento– sino un acceso vinculado al principio de finalidad. Corresponde al Departamento titular de la información asumir la responsabilidad de posibles infracciones, así como garantizar los derechos de acceso, rectificación y cancelación.

VI. LA SEGURIDAD DE LA INFORMACIÓN COMO GARANTÍA DE LA INTEGRIDAD, AUTENTICIDAD Y CONFIDENCIALIDAD EN LA ADMINISTRACIÓN ELECTRÓNICA

La Administración electrónica tiene que tener en cuenta especialmente el cumplimiento del principio de seguridad. En este caso, como los datos personales incorporados a la información administrativa van a ser sometidos a un tratamiento automatizado, es necesario respetar la normativa de seguridad de los ficheros automatizados que contengan datos de carácter personal. Esta normativa tiene como objeto establecer las medidas de índole técnica y organizativas necesarias que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado –art. 9 LOPD–. Por tanto, mientras el almacenamiento de datos personales en papel no estaba sujeto hasta ahora a unas concretas medidas de seguridad(195), estas medidas de seguridad siempre han existido

---

marco jurídico (por ejemplo, condición de acuerdo). Estas cuestiones se resolverían con frecuencia en el momento de la transposición de la Directiva sobre la firma electrónica al derecho nacional. En los casos restantes es imposible recurrir a proveedores externos privados, pues este papel está reservado al Estado (Alemania, España). En Francia, la cuestión funciona por defecto: hasta ahora, los operadores externos privados sólo intervienen en la certificación de la declaración del IVA en línea. En todos los casos restantes, el Estado actúa como autoridad certificadora.

(194) También tienen la consideración de encargados de tratamiento los operadores de telecomunicaciones que se encargan de la comunicación de datos entre el usuario de la red y el proveedor de acceso a Internet y los proveedores de acceso a Internet, que proporcionan, generalmente sobre la base de un contrato, una conexión TCP/I.

(195) El Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, contiene ya un conjunto de medidas de seguridad para los ficheros manual-estructurados –arts. 79-88 y 105-114–.

en el caso de los ficheros informatizados y son de plena aplicación a los tratamientos de datos personales en la Administración electrónica(196). Como hemos señalado en otro momento, las medidas de seguridad dependen sobre todo de la tipología de datos objeto de tratamiento, pudiendo ser de carácter básico, medio o alto(197). Esto es especialmente importante en los procedimientos de Administración electrónica donde se almacenen datos especialmente protegidos como ocurre en el ámbito de la salud –historias clínicas electrónicas–, de los servicios sociales –historias sociales en soporte electrónico–, o de la policía –expedientes para la prevención de un peligro para la seguridad pública y para la represión de infracciones penales–, que exigen la implantación de medidas de seguridad de nivel alto. También implica medidas de seguridad de nivel alto la participación social y la participación política por medios electrónicos(198), salvo que exista una voluntad de dar a conocer la propia opi-

(196) Estas medidas de seguridad se encontraban hasta ahora recogidas en el Real Decreto 994/1999, de 11 de junio, y ahora se encuentran en el Reglamento de desarrollo de la LOPD. El incumplimiento de las medidas de seguridad conlleva una infracción grave tal y como se establece en el artículo 44.3.h) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal –que no se ha visto modificado por la modificación del art. 44 de la LOPD por la Ley 2/2011, de 4 de marzo–. Cuando el tratamiento es parcialmente automatizado –o mixto –art. 56 del Reglamento–, es necesario implantar las medidas apropiadas a cada tipo de soporte. Esta cuestión la hemos analizado en nuestra «Introducción y Presentación» a *Seguridad y protección de datos personales*, Civitas-APDCM, Madrid, 2009, pp. 23-40.

(197) El Informe 327/2003, de la Agencia Española señala respecto a este punto: «Consideradas la direcciones IP como dato de carácter personal, de cara a la adopción de las medidas de seguridad que recoge el Real Decreto 994/1999 […] un fichero que contuviera únicamente las direcciones IP, en principio resultaría de aplicación las medidas de seguridad nivel básico. Por el contrario un fichero que contuviera la dirección IP asociada, por ejemplo, a los sitios web solicitados con la finalidad de elaborar un determinado perfil del usuario, si el mismo permite obtener una evaluación de la personalidad del individuo, se deberán adoptar las medidas de seguridad de nivel medio. Con ello queremos decir que, deberán implementarse sobre fichero los dispositivos técnicos que garanticen los niveles de seguridad que especifica el art. 4 del Reglamento, atendiendo a la naturaleza de la información tratada, y en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información». A nuestro juicio, si esta información está vinculada a la visita de determinados sitios web de carácter político, religioso o sexual, podrá merecer un nivel alto de protección. Esto es lo que ocurre con determinada información de los Proxy caché. La Agencia Española declaró que la Universidad de Castilla-La Mancha había cometido una infracción por un fallo de seguridad que permitió acceder por Internet al fichero con datos de acceso a direcciones web visitadas por los trabajadores de la Universidad.

(198) Así, la participación social implica en ocasiones una valoración política o ideológica. Éste es el caso, por ejemplo, de las votaciones al Consejo Asesor de la Guardia Civil. Otra solución es establecer que sea una participación anónima. De hecho, uno de los problemas –no el único– que presenta la participación política por medios electrónicos es el de la seguridad. Así, por una parte, es necesaria una identificación para la participación política y para poder efectuar el voto electrónico. Esto no presenta ningún inconveniente si el voto electrónico se efectúa en el Colegio donde se puede optar por mecanismos de identificación presencial. Sin embargo, el voto electrónico en el propio domicilio obliga a utilizar el DNI electrónico, lo que implica que el voto esté unido a la identificación.

nión política(199), como es el caso de la participación en foros de discusión de sitios web de las Administraciones Públicas cuando ésta no se hace de manera anónima. Especialmente compleja es la determinación del nivel de seguridad aplicable a las direcciones institucionales de correo electrónico y buzones electrónicos donde se reciben escritos, quejas, sugerencias y que admiten textos abiertos donde el ciudadano llega a incorporar información de diferente naturaleza, entre la que se pueden encontrar también datos que permitan establecer perfiles de personas, datos sobre infracciones administrativas, datos de salud, de ideología, de raza, etc.(200).

Por otra parte, la seguridad de la información tiene que garantizar el carácter secreto del sufragio. Así, a diferencia de nuestras relaciones electrónicas con la Agencia Tributaria, que deben ser confidenciales frente a terceros pero no frente a la propia Administración, en el ámbito del sufragio, la Administración electoral debe proceder a identificar al votante, pero no el contenido del voto –que debe ser secreto–, al tiempo que el votante debe tener la seguridad de que su sufragio ha sido emitido y es computado. La seguridad en la democracia electrónica debe garantizar también la calidad de los recuentos y la disponibilidad de la información, frente a ataques al servidor del sistema electoral por *hackers* que dificulten el recuento o lo manipulen. Téngase en cuenta que cualquier error del sistema de información invalidaría el proceso electoral en su conjunto y crearía graves problemas de confianza en el sistema político. Por tanto, las incertidumbres en materia de seguridad de la información y en términos de confianza son las causas de que no se introduzca de manera generalizada el voto electrónico en las elecciones políticas. Hay que mencionar que el sistema de voto electrónico se utiliza en Brasil desde 1996 y ha aportado ventajas en relación a la seguridad física del escrutinio y de las urnas y en la reducción de los votos nulos –a partir de 2014 el sistema de voto llevará incorporado en Brasil un lector biométrico de huellas dactilares–. En todo caso, sí existe una utilización generalizada de las nuevas tecnologías en el ámbito de la Administración electoral, por ejemplo, para la elaboración, mantenimiento actualizado y consulta del censo electoral. Cfr. A. J. Sánchez Navarro, «Sistema electoral y nuevas tecnologías: oportunidades y riesgos para la legitimación democrática del poder», *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, nº 1, 2005, pp. 83-109; y «Telemática y democracia», en J. Asensi Sabater (coord), *Ciudadanos e Instituciones en el Constitucionalismo actual*, Tirant lo Blanch, Valencia, 1997, pp. 363-383. Sobre la posibilidad de implantar el voto electrónico en España, cfr. también M. Carrillo, «Universal, libre e igual», *El País*, 3 de octubre de 2004; L. Cotino Hueso, «El voto electrónico o la casa por el tejado. La necesidad de construir la democracia y la participación electrónica por los cimientos», en L. Cotino Hueso (Coord.), *Libertades, democracia y gobierno electrónicos*, Comares, Granada, 2006, pp. 171 y 198.

(199) Como hemos señalado en otras ocasiones, no tiene sentido implantar medidas de seguridad de nivel alto a los ficheros donde se hace referencia a que un representante político o sindical pertenece a un partido político o a un sindicato porque es una información que el interesado ha hecho manifiestamente pública –art. 8.2.e) de la Directiva 95/46/CE– y se encuentra en distintas fuentes accesible al público como medios de comunicación y boletines oficiales.

(200) El Reglamento de desarrollo de la LOPD mantiene para los ficheros manual-estructurados la misma tipología de datos a la hora de exigir la implantación de medidas de seguridad de nivel básico, medio y alto, si bien establece expresamente que no es necesario aplicar a estos ficheros las medidas de seguridad de nivel alto cuando «se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad» [art. 81.5.b)]. De esta forma, el hecho de que exista un dato especialmente protegido no obliga a implantar medidas de seguridad

La seguridad de la información es especialmente importante en el ámbito de la Administración electrónica ya que es una garantía de la integridad y autenticidad de los datos personales y, por tanto, del cumplimiento del principio de calidad como principio de exactitud(201). De esta forma, la implantación de medidas de seguridad permite la conservación de la información administrativa y evita la alteración de la documentación contenida en los ficheros administrativos, tanto de la aportada por los interesados como de aquella elaborada por la Administración, lo que es imprescindible para la tutela de los derechos y para el normal funcionamiento de la actividad administrativa ya que no es posible asumir la validez de un documento administrativo si no se encuentra garantizada su autenticidad y su integridad(202). También el principio de seguridad es una garantía de la disponibilidad de la información, algo esencial ya que los derechos de las personas se ejercen a través de su información personal sometida a tratamiento y se ven afectados por la denegación del servicio –la *denial of service*– de los sistemas de información(203). Como hemos señalado en otro momento, la protección de datos personales no sólo es un derecho autónomo sino una garantía institucional de otros derechos. Esto se evidencia especialmente en el cumplimiento del principio de seguridad en la Administración electrónica ya que la falta de inte-

---

de nivel alto si este dato es accesorio o incidental en relación con la finalidad, un criterio que podría utilizarse en este caso pero que, sin embargo, no está previsto para los tratamientos automatizados. No parece razonable que el nivel de seguridad tenga que depender del tipo de dato que el ciudadano incluya en cada caso en un escrito dirigido a un buzón electrónico si la finalidad principal de éste no es el tratamiento de datos especialmente protegidos. Lo más aconsejable en términos de garantía del derecho es tratar de disociar la información cuando no sea imprescindible para la finalidad. Si es necesario que la información se mantenga asociada a una persona física, lo aconsejable es implementar medidas de seguridad de nivel alto o, en el caso de que no sea posible, informar al ciudadano de que las medidas de seguridad son de nivel básico o de nivel medio, de forma que no incorpore información que exija un mayor nivel de seguridad. En ningún caso la implementación de medidas de seguridad en el fichero puede hacerse depender de cada tipo de escrito y mucho menos debe configurarse un tratamiento inteligente que en virtud de un tipo de palabras establezca el nivel de seguridad porque esto vulneraba el principio de proporcionalidad en sentido estricto.

(201) El Grupo del Artículo 29 en el documento ya citado sobre Administración en línea resalta que todas las Autoridades de protección de datos insisten especialmente en la cuestión de la seguridad de datos y en la necesidad de garantizar un nivel satisfactorio de seguridad de las aplicaciones correspondientes.

(202) Hay medidas de seguridad establecidas en el Reglamento de desarrollo de la LOPD que están dirigidas a garantizar la integridad de la información frente a pérdidas accidentales de información o manipulaciones indebidas, como la existencia de copias de respaldo y recuperación que permiten la reconstrucción y la recuperación de los datos, copias que deben conservarse en un lugar diferente de aquel en el que se encuentren los equipos informáticos.

(203) Esta denegación de servicio proviene no sólo de incidentes fortuitos sino también de ataques a los sistemas de información de una organización. Por ello, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, señala que los registros electrónicos podrán rechazar los documentos electrónicos que se les presenten, que contengan código malicioso o dispositivo susceptible de afectar a la integridad o seguridad del sistema.

gridad y disponibilidad de la información afecta principalmente al ejercicio de derechos. Así, por ejemplo, la pérdida o la alteración de la historia clínica o su falta de disponibilidad perjudican la asistencia(204). También es importante la seguridad como garantía de la confidencialidad, al impedir que los tratamientos se conviertan en cesiones indiscriminadas de datos personales, evitando los accesos indebidos por parte de terceras personas, especialmente en las comunicaciones realizadas entre los ciudadanos y la Administración y entre las propias Administraciones Públicas(205). Los procesos de centralización de la información administrativa –historial académico electrónico, historia clínica electrónica, receta electrónica–, si bien también generan riesgos, suponen un importante avance para la implantación, seguimiento y auditoría de las medidas de seguridad que impone la normativa. En todo caso, cualquier proyecto de Administración electrónica debe tener especialmente presente la necesidad de

(204) La Agencia de Protección de Datos declaró una infracción grave prevista en el artículo 44.3.d) de la LOPD a una dirección de un centro sanitario por una falta de disponibilidad de una historia clínica de un menor inmigrante durante un año que impedía que ésta fuera consultada por su pediatra, a pesar de sucesivas reclamaciones de los representantes legales del menor, con las repercusiones que esto podía suponer para el derecho a la asistencia sanitaria de un menor extranjero en régimen de acogimiento. No existía, en este caso, una pérdida de datos, sino la «carencia de medidas organizativas en relación con las necesarias indicaciones a la pediatra de la menor para el adecuado acceso al contenido íntegro de la historia clínica de ésta». La mejora en la definición del tipo previsto en el antiguo art. 44.3.d) LOPD a través del nuevo art. 44.3.c), que ha realizado la Ley 2/2011, de 4 de marzo, de Economía Sostenible obliga ahora a calificar los hechos descritos dentro del art. 44.3.h) –incumplimiento de medidas de seguridad–, que también es una infracción grave.

(205) Por ello, es especialmente importante que los servicios de Administración electrónica cuenten con sistemas adecuados de identificación y autenticación que acrediten, de manera inequívoca, la identidad del interesado y la autenticidad de los datos y documentos aportados. Además, el uso de medios abiertos de transmisión de datos obliga al responsable del tratamiento a implantar medidas de seguridad en los sistemas de comunicaciones para evitar que la información se pierda o sea alterada o interceptada por quien no sea su legítimo destinatario. Entre las medidas de seguridad de nivel alto se encuentra el cifrado que se aplica al uso de redes públicas de telecomunicaciones (Internet, RDSI) pero no al uso de redes privadas. En el ámbito de las Administraciones Públicas, el titular de la red garantiza en ocasiones al responsable del fichero el uso privativo de redes públicas, es decir, la existencia de una red privada virtual, lo que plantea la posibilidad de exceptuar el cifrado. Históricamente, se han dado en las Administraciones Públicas situaciones de sobre-clasificación de ficheros –que no necesariamente tenían que ser de nivel alto–, lo que obligaba a cifrar las comunicaciones y ralentizaba la gestión. La mejora de la tecnología ha resuelto la mayoría de los problemas que se presentaban hace años. El art. 34 de la Ley General de Telecomunicaciones –titulado «Protección de los datos de carácter personal»– establece que los operadores «deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar los niveles de protección de los datos de carácter personal que sean exigidos por la normativa de desarrollo de esta Ley en esta materia. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar».

establecer niveles de acceso(206). Así, de entre las medidas de seguridad que hay que implantar en la Administración electrónica es muy importante el cumplimiento de aquellas medidas de seguridad que permiten que sólo accedan a la información las personas autorizadas –por ejemplo, el trabajador social o el facultativo que presta la asistencia al usuario– y no otras personas. Entre estas medidas hay que destacar el control de accesos –que obliga al establecimiento de una relación de personas autorizadas con acceso a los datos–, la implantación de medidas de identificación y autenticación –lo que permite que los usuarios autorizados tengan acceso únicamente a aquellos datos y recursos para el desarrollo de sus funciones(207)– y el registro de accesos –que facilita la trazabilidad de la información de cada acceso(208)–. No olvidemos que el art. 9.3 de la LOPD hace referencia a los requisitos que deben reunir las personas que intervengan en el tratamiento de los datos(209). Es importante que en los proyectos de Administración electrónica se valore la necesidad de implementar las medidas de seguridad técnicas en el momento del diseño de la aplicación –*privacy by design*– y no posteriormente.

La normativa administrativa ha obligado tradicionalmente a las Ad-

(206) Por ejemplo, el uso de la red como repositorio de información sanitaria básica individual o para enviar información sanitaria exige que sólo pueda acceder a esa información aquél que está autorizado para ello, de manera que se asegure la identidad y confidencialidad. Lo mismo ocurre cuando se establece un modelo de publicación restringida –en una Intranet o en un espacio privado en Internet– para que sólo tengan acceso a la información aquellas personas que ostenten un interés legítimo, de forma que el establecimiento de medidas de seguridad evite el acceso a personas no autorizadas. Cfr. nuestro trabajo «Transparencia administrativa y protección de datos personales», cit., pp. 64-66.

(207) El Reglamento de desarrollo de la LOPD dispone como medida de seguridad de nivel básico el control de acceso, señalando que «los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones». Por lo tanto, el responsable del fichero «establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados» (art. 91). El control de acceso físico es una medida de seguridad de nivel medio cuya implantación exige el Reglamento de desarrollo de la LOPD (art. 99): «Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información».

(208) Es especialmente importante el registro de accesos que permita que de cada acceso se guarde como mínimo la identificación del usuario, la fecha y la hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Sin embargo, de poco sirve el registro de accesos si el responsable de seguridad no revisa periódicamente la información.

(209) Es necesario señalar que el personal que atiende la sede electrónica o el registro telemático no debe acceder, en ningún caso, al contenido de los datos o documentos aportados por el ciudadano, distintos de aquellos que identifiquen al solicitante, la solicitud realizada y el órgano competente para su resolución. Tampoco las personas que atiendan los repositorios de datos o documentales deben acceder, en ningún caso, al contenido de los datos o documentos que en el mismo se incorporen, limitando su tratamiento a poner a disposición de los órganos administrativos solicitantes la información requerida, verificando previamente que disponen del consentimiento del interesado para poder facilitar esa información.

ministraciones Públicas a adoptar medidas técnicas y organizativas necesarias que aseguren la identidad, autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información cuando utilicen soportes, medios y aplicaciones electrónicas, informáticas y telemáticas para la iniciación, tramitación y terminación de los procedimientos administrativos(210). Hay que destacar que la LAECSP es muy precisa en lo que respecta a la seguridad de la información. Así, reconoce como un derecho de los ciudadanos «la garantía de la seguridad y la confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas» –art. 6.2.I)– y establece como uno de sus fines la creación de «condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos» –art. 3.3–. De hecho, un objeto de esta Ley es que las Administraciones Públicas utilicen las tecnologías de la información «asegurando […] la integridad, la autenticidad, la confidencialidad y la conservación de los datos» –art. 1.2–. La LAECSP insiste que las transmisiones de datos entre Administraciones Públicas –que permiten al ciudadano no aportar datos y documentos que estén en poder de las Administraciones Públicas– se hará «especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo» –art. 9.1–. La LAECSP señala que el principio de proporcionalidad implica modular las garantías y medidas de seguridad a la naturaleza y circunstancias de los distintos trámites y actuaciones –art. 4.g)–. Estas medidas de seguridad deben adaptarse especialmente a la tipología de datos sometidos a tratamiento como así establece la normativa relativa a las medidas de seguridad en el tratamiento de los datos de carácter personal –que se encuentra descrita en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre–, sin perjuicio de que la normativa reglamentaria que desarrolle la LAECSP –especialmente

(210) Así, por ejemplo, el art. 38.9 de la LRJAP y PAC exigía que los registros telemáticos cumplan los criterios de disponibilidad, autenticidad, integridad, confidencialidad y conservación de la información. Igualmente, el art. 45.3 añadía que «[l]os procedimientos que se tramiten y terminen en soporte informático garantizarán la identificación y el ejercicio de la competencia por el órgano que la ejerce». El art. 45.5 señala que «[l]os documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras leyes». Estos dos preceptos han sido derogados por la LAECSP.

el Esquema Nacional de Seguridad– pueda valorar la naturaleza y circunstancias de los distintos trámites(211).

Es muy importante destacar en este punto la regulación que la LAECSP lleva a cabo de las distintas formas de identificación y autenticación. Así, establece que las Administraciones Públicas admitirán en sus relaciones por medios electrónicos los sistemas de firma electrónica conformes con lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica(212) y que resulten adecuados para «garantizar la

(211) El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, establece en el art. 5.3 que las condiciones de identificación de las sedes electrónicas y de seguridad de sus comunicaciones se regirán, además de por lo dispuesto en ese Real Decreto, por lo previsto en el Título VIII del Reglamento de desarrollo de la LOPD. No obstante, ese Real Decreto también prevé la existencia de dos instrumentos, que la Exposición de Motivos define como «de carácter técnico y complementario»: el Esquema Nacional de Interoperabilidad, encargado de establecer los criterios comunes de gestión de la información que permitan compartir soluciones e información, y el Esquema Nacional de Seguridad, que deberá establecer los criterios y niveles de seguridad necesarios para los procesos de tratamiento de la información que prevé el propio Real Decreto. Así, se establece –art. 5.4– que los sistemas de información que soporten las sedes electrónicas deberán garantizar la confidencialidad, disponibilidad e integridad de las informaciones que manejan. Mientras que no se aprueben estos esquemas, la Disposición Transitoria Cuarta del Real Decreto 1671/2009, de 6 de noviembre, señala que la creación de sedes electrónicas deberá ir acompañada de un informe en el que se acredite el cumplimiento de las condiciones de confidencialidad, disponibilidad e integridad de las informaciones y comunicaciones que se realicen a través de las mismas. Finalmente el Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica han sido aprobados respectivamente por los Reales Decretos 3/2010 y 4/2010, ambos de 8 de enero. En el ámbito de las Comunidades Autónomas, hay que destacar tempranamente el Decreto 175/2002, de 14 de noviembre, del Consejo de Gobierno de la Comunidad de Madrid por el que se regula la utilización de las técnicas electrónicas, informáticas y telemáticas por esta Administración que establece expresamente la «necesidad de contar con medidas de seguridad que garanticen la integridad, autenticidad, protección y conservación de los documentos almacenados, y en particular, la de asegurar la identificación de los usuarios y el control de accesos para asegurar la confidencialidad e integridad de los datos tratados por la aplicación, de conformidad con las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, así como en aquellas normas de desarrollo que sean aplicables».

(212) Existe una clara apuesta por la firma electrónica en las comunicaciones administrativas. Esta firma electrónica es un código matemático complejo, una mezcla de una clave privada y una clave pública que permite conocer la identidad de la persona que envía o recibe ese mensaje y también garantiza, a través de un procedimiento de encriptado y desencriptado, la integridad y la confidencialidad de esa información. Son los prestadores de servicios de certificación los que expiden estos documentos electrónicos que relacionan la firma electrónica de cada usuario con su identidad personal. El Documento Nacional de Identidad electrónico, que es un certificado electrónico reconocido, es capaz de acreditar la identidad, integridad y confidencialidad. La Ley 59/2003, de 19 de diciembre, reguló la firma electrónica. No obstante, hubo enfrentamiento entre los posibles certificadores «privados» –Cámaras de Comercio a través de Camerfirma, Notarios y Registradores, Telefónica, etc.– frente a la Fábrica Nacional de Moneda y Timbre. La utilización de la firma electrónica se utiliza

identificación de los participantes, y, en su caso, la autenticidad e integridad de los documentos electrónicos –art. 13.1»(213). De esta forma, los ciudadanos pueden utilizar para relacionarse con la Administración los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, los sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas(214) y otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen –art. 13.2 LAECSP–(215). Hay que destacar especialmente que

---

más en las relaciones con la Administración y poco en el tráfico ordinario de la empresa –límites cuantitativos–. Esta Ley señala en el art. 4 que la firma electrónica se aplicará en el seno de las Administraciones Públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares. Cfr. también el Decreto 94/2006, de 8 de noviembre, del Consejo de Gobierno, de utilización de la firma electrónica en las relaciones con la Administración de la Comunidad de Madrid por medios electrónicos, informáticos y telemáticos.

(213) La Ley 59/2003, de 19 de diciembre, de Firma Electrónica señala tres tipos de firma electrónica: la firma electrónica simple –conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante–; la firma electrónica avanzada –la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control–; y la firma electrónica reconocida –que es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel–.

(214) Posteriormente se señala que la Administración General del Estado dispondrá, al menos, de una plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de las Administraciones Públicas que será de libre acceso por parte de todos los Departamentos y Administraciones. Esta Plataforma de verificación de certificados y el sistema nacional de verificación han sido regulados en el art. 25 del Real Decreto del 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007. El documento ya citado del Grupo del Artículo 29 afirma que los procedimientos de administración en línea en el sector de las finanzas públicas se caracterizan por un nivel de seguridad más elevado, pues varios países declaran contar con sistemas de firma electrónica como Finlandia, España, Francia, o de cifrado de datos como Francia, Portugal, España.

(215) El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, señala en su Exposición de Motivos que en materia de identificación y autenticación ha pretendido establecer los elementos mínimos imprescindibles para afianzar «el criterio de flexibilización impulsado en la LAECSP que, junto a la admisión como medio universal de los dispositivos de identificación y firma electrónica asociados al Documento Nacional de Identidad, admite la utilización de otros medios de autenticación que cumplan con las condiciones de seguridad y certeza necesarias para el normal desarrollo de la función administrativa». Es positivo que la LAECSP permita los sistemas de firma débil para gestiones administrativas sencillas que no requieren una especial manifestación de voluntad con efectos jurídicos relevantes como es el caso de la petición de datos tributarios, de una nómina o de una cita médica, que no de-

la firma electrónica avanzada basada en un certificado reconocido autentifica al ciudadano –asegura su identidad–, impide el no repudio, asegura la integridad del documento firmado y evita el acceso por personas no autorizadas, por lo que es una poderosa herramienta para garantizar la seguridad de la información(216).

La LAECSP incide en la importancia de la seguridad de la información dentro de la Administración electrónica, que cobra una especial relevancia en la comunicación del ciudadano con la Administración en el marco de un procedimiento administrativo y cuando éste va a incorporar documentación que va a producir efectos jurídicos(217). El derecho a conocer por medios electrónicos el estado de tramitación de los procedimientos en los que se tenga la condición de interesados y a obtener copias electrónicas de los documentos electrónicos que formen parte del expediente requiere mecanismos de identificación y autenticación fuerte. Así, al regular la sede electrónica, señala que su establecimiento «conlleva la responsabilidad del titular [de la sede electrónica] respecto de la inte-

---

ben exigir un sistema de identificación y autenticación como el DNI electrónico sino que deben poder hacerse a través de una clave que se cambie periódicamente o aportando un dato conocido por ambas partes –número de una determinada casilla, número de matrícula de la Universidad, número de la seguridad social–. El Real Decreto 1671/2009, de 6 de noviembre, «ha previsto un régimen específico que facilita la actuación en nombre de terceros a través de dos mecanismos fundamentales: por un lado, la figura de las habilitaciones generales y especiales, pensadas fundamentalmente para el desempeño continuado y profesional de actividades de gestión y representación ante los servicios de la Administración, así como un registro voluntario de representantes, también pensado con la finalidad de facilitar el ejercicio de la función de representación, estableciendo un mecanismo de acreditación en línea del título previamente aportado a dicho registro».

(216) También las Administraciones Públicas pueden utilizar distintos sistemas de firma electrónica para la identificación electrónica y autenticación de los documentos electrónicos que produzcan: sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y con ella el establecimiento de comunicaciones seguras; sistemas de firma electrónica para la actuación administrativa automatizada; firma electrónica del personal al servicio de las AA.PP.; intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes –art. 13.3 LAECSP–.

(217) Igualmente, el art. 96.5 de la Ley General Tributaria señala que «los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por la Administración tributaria, o los que ésta emita como copias de originales almacenados por estos mismos medios, así como las imágenes electrónicas de los documentos originales o sus copias, tendrán la misma validez y eficacia que los documentos originales, siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por la normativa aplicable». Igualmente, el Real Decreto 1671/2009, de 6 de noviembre, en su Exposición de Motivos señala que la relevancia jurídica de la actividad administrativa ha exigido prestar una atención singularizada al uso de los medios de identificación y autenticación electrónica por parte de la Administración, estableciendo la necesidad de incorporación de sellos o marcas de tiempo, que acrediten la fecha de adopción de los actos y documentos que se emitan. Igualmente se ha dispensado una atención especial a la autenticación en el seno de la actuación automatizada.

gridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma» –art. 10.1–(218), un aspecto que también resalta la Exposición de Motivos –apdo. VI–(219). Igualmente se señala que cada Administración Pública determinará las condiciones e instrumentos de creación de sedes electrónicas, con sujeción, entre otros, al principio de seguridad –art. 10.2–(220). Además, las sedes electrónicas «utilizarán, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente» –art. 17 LAECSP–. Los registros electrónicos también deberán contar «con las medidas de seguridad necesarias para garantizar su integridad» –art. 26.1(221). Esto se

(218) El art. 7 del Real Decreto 1671/2009, de 6 de noviembre añade que el titular de la sede electrónica que contenga un enlace o vínculo a otra cuya responsabilidad corresponda a distinto órgano o Administración Pública no será responsable de la integridad, veracidad ni actualización de esta última. La sede establecerá los medios necesarios para que el ciudadano conozca si la información o servicio al que accede corresponde a la propia sede o a un punto de acceso que no tiene el carácter de sede o a un tercero. En todo caso, los órganos u organismos públicos titulares de las sedes electrónicas compartidas responderán por sus contenidos propios y solidariamente por los contenidos comunes.

(219) Sin embargo, se echa en falta una referencia a medidas de seguridad concretas a implantar en las oficinas de atención presencial que ponen a disposición de los ciudadanos, de forma libre y gratuita, medios e instrumentos precisos para garantizar el acceso de todos los ciudadanos a los servicios electrónicos –art. 8.2.a) LAECSP–. Estos puestos de acceso electrónico, al no ser personales, deben disponer de las necesarias medidas de seguridad como el no almacenamiento en disco de contraseñas de identificación, el borrado automático de los archivos descargados al finalizar la sesión, etc. Así, se pueden tener en cuenta en estos puntos los mismos criterios que deben ser de aplicación para los centros de acceso público a Internet. Estos centros de acceso público a Internet han adoptado medidas para garantizar el cumplimiento de las normas de utilización, especialmente en cuanto a no acceder a sitios con contenido pornográfico, de incitación a la violencia, racismo o terrorismo. Sin embargo, al mismo tiempo estos centros deben garantizar la confidencialidad de estos accesos así como de los datos que los usuarios transmitan en sus conexiones con Internet. Por ello, no parece adecuado el análisis de los accesos realizados por cada usuario que habrán sido grabados en un archivo histórico por el servidor de acceso a Internet (proxy), que deja constancia de los accesos de cada usuario, con la dirección de Internet accedida. Cada vez que un usuario concluya una sesión de conexión a Internet deberán eliminarse las cachés de información generados durante la navegación así como las *cookies* que hayan podido almacenarse en el equipo. Lo adecuado es utilizar filtros que impiden el acceso a determinados sitios de Internet. En ningún caso debe grabarse los contenidos de los formularios de páginas de Internet, o correos electrónicos que envíe el usuario ni utilizarse productos que permitan visualizar los contenidos de los mensajes que esté enviando o recibiendo cada usuario. Cfr. sobre esta cuestión A. SÁNCHEZ NAVARRO, «La articulación del derecho a la protección de datos de carácter personal», *loc. cit.*, p. 110.

(220) El art. 10.4 de la LAECSP señala que las sedes electrónicas «dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias».

(221) El Real Decreto 1671/2009, de 6 de noviembre, señala que el registro electrónico emitirá automáticamente un recibo firmado electrónicamente, copia del escrito, comunicación o solicitud presentada, fecha y hora de presentación y número de entrada de registro, en su caso enumeración y denominación de los documentos adjuntos al formulario de presentación o documento presentado, seguida de la huella electrónica de cada uno de ellos e información del plazo máximo establecido normati-

aplica igualmente al régimen de copias electrónicas. Así, las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que «garanticen su autenticidad, integridad y la conservación del documento imagen» –art. 30.3. Este principio también tiene plena aplicación en el archivo electrónico de documentos, ya que los «medios o soportes en que se almacenan documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados» –art. 31.3–. De hecho, este precepto exige en particular dos medidas de seguridad, la identificación de los usuarios y el control de acceso, así como el cumplimiento de las garantías previstas en la legislación de protección de datos –art. 31.3–. Igualmente, el foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico firmado por la Administración, índice que garantizará «la integridad del expediente electrónico y permitirá su recuperación, siempre que sea preciso» –art. 32.2–. También establece que «deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan» –art. 20.4–. Los requerimientos de seguridad también se aplican a las comunicaciones electrónicas(222). Así, las comunicaciones electrónicas sólo serán válidas si existe constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifica fidedignamente al remitente y al destinatario –art. 27.3–. Expresamente se indica que los «requisitos de seguridad e integridad de las comunicaciones se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquéllas, de acuerdo con los principios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal» –art. 27.5–. Así, en relación con la interoperabilidad de los sistemas de información, se establece que las Administraciones Públicas utilizarán tecnologías de la información en sus relaciones con los ciudadanos y con el resto de Administraciones Públicas aplicando medidas de seguridad –art. 41–.

---

vamente para la resolución y notificación del procedimiento, así como de los efectos que pueda producir el silencio administrativo, cuando éste sea automáticamente determinable –art. 30–.

(222) Un factor de riesgo es la utilización de conexiones electrónicas por Internet, lo que conlleva la intervención de una pluralidad de agentes en las distintas fases del proceso. La Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que deroga la anterior Directiva 97/66/CE, ha limitado sus referencias a Internet a los Considerandos 6 y 25 y al art. 5.3. La Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) ya citada, incide en la importancia de «los instrumentos de cifrado que impiden el pirateo de la información transmitida por Internet [que] responden a la obligación del responsable del tratamiento de datos de adoptar medidas adecuadas para proteger los datos personales frente al tratamiento ilícito».

Es de enorme importancia la seguridad para dar confianza en las relaciones entre los ciudadanos con las Administraciones públicas por medios electrónicos. En todo caso, esta voluntad de emplear la firma electrónica para garantizar la identidad, autenticidad e integridad de los documentos electrónicos demuestra que las tecnologías de la información y, más en concreto, la Administración electrónica es una oportunidad estratégica para fortalecer también la seguridad y la confidencialidad de la información administrativa(223), mejorando la custodia del almacenamiento y de la remisión de la información en papel que era muy difícil de gestionar(224), cuya confidencialidad dependía, en muchas ocasiones, del cumplimiento del deber de secreto(225) por parte de los empleados públicos –art. 10 LOPD–(226). Está claro que la migración de un soporte papel a un soporte automatizado supone un notable incremento de las medidas de seguridad. Incluso, las formas de identificación y autenticación previstas en la LAECSP suponen una mejora de la seguridad –de la integridad y de la confidencialidad, especialmente del no repudio– en relación con la identificación por nombre, número de DNI y contraseña que se utilizaba hasta ahora en los medios electrónicos. Lógicamente, la implantación de medidas de seguridad en la Administración electrónica tiene que respetar también aquí el principio de neutralidad tecnológica(227).

---

(223) La Ley 59/2003, de 19 de diciembre, de Firma Electrónica establece en su Exposición de Motivos que dicha firma «surge como respuesta a la necesidad de conferir seguridad a las comunicaciones por Internet», convirtiéndose de este modo en un instrumento generador de confianza en las comunicaciones telemáticas y en un dinamizador de la Administración y el comercio electrónicos, al elevar los niveles de seguridad garantizando la identidad de los comunicantes, la autenticidad de las comunicaciones y la integridad de los contenidos.

(224) Recuérdese todos los problemas que supone el abandono en la calle de historias clínicas o de expedientes judiciales en papel y la alarma social que genera y que se traslada a los medios de comunicación.

(225) Si el incumplimiento del deber de secreto era antes una infracción leve –antiguo art. 44.2.e) LOPD, salvo las previsiones establecidas para los ficheros a los que le corresponde un nivel medio y alto de sguridad–, la Ley 2/2011, de 4 de marzo, de Economía Sostenible, a través de su Disposición final quincuagésima sexta, ha modificado su calificación, que pasa a ser considerada una infracciñón grave –nuevo art. 44.3.d)–.

(226) La LAECSP comete, a nuestro juicio, un error cuando al proclamar el principio de seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, señala que «se exigirá al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa» –art. 4.f)– ya que en el momento de entrada en vigor de esta Ley no existían medidas de seguridad aprobadas para los ficheros en papel. Además, hay medidas de seguridad que sólo se pueden implantar en un soporte automatizado –como los mecanismos de identificación y autenticación que implican el bloqueo ante intentos reiterados de acceso, las copias de respaldo y recuperación o el cifrado en la distribución de soportes y en las telecomunicaciones– y otras muchas medidas –como el registro de accesos– son más fáciles de implementar en los tratamientos automatizados.

(227) Es interesante la reflexión de Sánchez Navarro para quien la utilización del *software* libre permite una mayor seguridad ya que dificulta la posibilidad de introducir programas de control remoto «que, al incluir accesos secretos al *software*, pueden visualizar o borrar datos, conseguir contra-

VII. EL EJERCICIO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN ELECTRÓNICA Y LAS COMPETENCIAS DE LAS AUTORIDADES DE CONTROL

Los proyectos de Administración electrónica deben tener presente la necesidad de garantizar los derechos de acceso, oposición, rectificación y cancelación de los interesados sobre sus datos personales almacenados en los distintos procedimientos administrativos(228). Las nuevas tecnologías, lejos de ser un obstáculo, se presentan como aliadas ya que facilitan también el ejercicio de estos derechos, incluso la propia tutela de una autoridad de control, a través de medios electrónicos. Si, como hemos señalado antes, la implantación de la Administración electrónica supone un incremento de los tratamientos de datos personales, una forma de equilibrar esta injerencia en el derecho a la protección de datos es permitir también a través de medios electrónicos el ejercicio de los derechos de acceso, rectificación, cancelación y oposición(229), de forma que se facilite el control sobre la propia información personal(230). Para ello es

---

señas, etcétera, poniendo así en peligro la privacidad de estos datos, cuestión totalmente transparente para los programadores "libres" que, al conocer el código fuente podrían sin dificultad revisar y comprobar que no se han introducido este tipo de controles remotos». Cfr. A. SÁNCHEZ NAVARRO, *loc. cit.,* pp. 112-113.

(228) En la Resolución 400/2006 –ya citada–, la Agencia Española ha reconocido el derecho de acceder a información relativa a la dirección o direcciones IP asignadas a las conexiones a Internet así como a los datos de tráfico adicionales disponibles, una resolución que, si bien no se refiere a la Administración electrónica, sí puede tener algunas implicaciones en ella. El contenido de este derecho comprende los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos. En ese momento el art. 12 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (en lo sucesivo LSSI), obligaba a los operadores de redes y proveedores de acceso a retener los datos de conexión por un período máximo de doce meses. La Agencia dictó una resolución de tutela de derechos porque la solicitud no fue atendida en plazo por el responsable del fichero. Aun en el caso de que los datos hubieran sido cancelados, la operadora debió informar sobre el protocolo que rige su actuación, de modo que fuera posible concretar si dicha cancelación ya se había producido cuando la reclamante presentó su solicitud o si la misma tuvo lugar con posterioridad, en cuyo caso la conducta mantenida por la operadora podría ser constitutiva de infracción administrativa, al haber impedido u obstaculizado el ejercicio de los derechos que la LOPD atribuye a la reclamante. En ese caso, la empresa había reconocido expresamente que los datos solicitados no habían sido destruidos, sino que se encontraban bloqueados a disposición de las Administraciones Publicas, Jueces y Tribunales.

(229) La Ley 2/2011, de 4 de marzo, de Economía Sostenible a través de su Disposición final quincuagésima sexta, ha modificado la LOPD al establecer que el impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición es una infracción grave –nuevo art. 44.3.e)–, cuando con anterioridad, no atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales era una infracción leve –antiguo art. 44.2.a)–.

(230) Como hemos indicado antes, la Agencia de Protección de Datos de la Comunidad de Madrid impulsó una aplicación de ejercicio telemático de derechos de protección de datos (DEPD) que facilita a los ciudadanos los derechos de acceso, rectificación y cancelación ante el responsable del

necesario que en el diseño de un servicio de Administración electrónica donde se proceda al tratamiento de datos personales se implemente la posibilidad de que en cualquier momento el interesado pueda ejercitar los derechos de acceso, rectificación, oposición y cancelación por medios electrónicos a través de un *link*, identificando claramente el centro directivo que es responsable del tratamiento y ante el cual se están ejercitando estos derechos. No tiene mucho sentido ofrecer a los ciudadanos un acceso electrónico a los procedimientos administrativos y no reconocer al mismo tiempo el ejercicio de los derechos de acceso, rectificación, cancelación y oposición también por medios electrónicos. Por tanto, tiene que facilitarse el ejercicio de estos derechos en los registros electrónicos, en los repositorios de información personal, en la publicación de datos personales en Boletines o Diarios Oficiales a través de Internet o en sitios webs institucionales(231) y en todos los servicios electrónicos prestados a los ciudadanos que impliquen tratamientos de datos personales –servicios de alertas y noticias, foros de participación social por medios electrónicos, sistemas de sugerencias y reclamaciones, etc.–.

La LAECSP proclama el derecho a «conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquéllos» –art. 6.2.d)–. También señala que «[e]n los procedimientos administrativos gestionados en

---

fichero de la Administración de la Comunidad de Madrid a través de Internet. Igualmente, esta herramienta permite la solicitud de tutela de estos derechos por vulneraciones del responsable así como la formulación de denuncias por incumplimiento de la legislación de protección de datos ante la Agencia de Protección de Datos de la Comunidad de Madrid, también a través de Internet. El acceso a la herramienta debe realizarse acreditando inequívocamente la identidad del ciudadano mediante certificado digital válido y reconocido. Cfr. «Presentación» a *Memoria de la Agencia de Protección de Datos de la Comunidad de Madrid 2007*, pp. 343-346–.

(231) Hemos analizado en otro momento la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición en relación a los tratamientos de datos personales que se producen con su publicación en Boletines o Diarios Oficiales a través de Internet o en sitios webs institucionales. Así, por ejemplo, se puede ejercer el derecho de oposición a la publicación de los datos personales porque el responsable ha determinado un nivel de publicidad que supone una injerencia excesiva en el derecho fundamental a la protección de datos personales –cuando el fin público que justificaba la publicidad podría alcanzarse con un menor nivel de publicidad como aquella que se realiza en una Intranet o en un espacio privado en Internet–, porque la publicación contiene datos excesivos o porque se mantiene la publicación habiendo finalizado el plazo dentro de la cual era necesaria, convirtiéndose así en un tratamiento excesivo. El órgano administrativo que ordenó la publicación de los datos de carácter personal en el boletín o en el sitio web institucional deberá atender las solicitudes de ejercicio de los derechos, lo que obliga a que estos tratamientos de datos personales se lleven a cabo de una manera que lo permita. El órgano administrativo responsable de ordenar la publicación deberá justificar su denegación al interesado, con expresa mención del precepto legal en el que se ampare, informándole de su derecho a recabar la tutela de una Agencia de Protección de Datos. Esta cuestión la hemos analizado en «Transparencia administrativa y protección de datos personales», cit., pp. 101-112.

su totalidad electrónicamente, el órgano que tramita el procedimiento pondrá a disposición del interesado un servicio electrónico de acceso restringido donde éste pueda consultar, previa identificación, al menos la información sobre el estado de tramitación del procedimiento [...]. La información sobre el estado de tramitación del procedimiento comprenderá la relación de los actos de trámite realizados, con indicación sobre su contenido, así como la fecha en la que fueron dictados. En el resto de los procedimientos se habilitarán igualmente servicios electrónicos de información del estado de la tramitación que comprendan, al menos, la fase en la que se encuentra el procedimiento y el órgano o unidad responsable» –art. 37–. La LAECSP también reconoce el derecho a «obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado» –art. 6.2.e)–. La LAECSP no ha previsto el acceso de terceros interesados a un procedimiento administrativo electrónico. Tampoco ha establecido el acceso electrónico a expedientes administrativos que correspondan a procedimientos terminados –art 37.1 LRJAP y PAC–. Ya hemos señalado en otro momento la deficiente regulación que tiene en nuestro país el derecho de acceso a información administrativa(232). Obviamente, no le correspondía a la LAECSP, que sólo modifica la LRJAP y PAC en aspectos básicamente instrumentales o adjetivos, modificar las exigencias de ésta, especialmente en lo que respecta a tener que ostentar un interés legítimo para el acceso a datos nominativos.

En todo caso, hay que recordar que el derecho de acceso regulado en el art. 15 de la LOPD es distinto al derecho de acceso a archivos y registros administrativos del art. 105.b) de la CE, desarrollado en la LRJAP y PAC–(233). El derecho de acceso regulado en el art. 15 de la LOPD permite al interesado «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». De esta manera, el derecho de acceso del art. 15

(232) Cfr. «Transparencia administrativa y protección de datos personales», cit., pp. 24-61.

(233) La LRJAP y PAC, que regula el acceso a archivos y registros administrativos y la LORTAD –posteriormente la LOPD–, que desarrolla el derecho fundamental a la protección de datos personales, a pesar de ser aprobadas en el mismo año, fueron dos leyes que se desconocen entre sí. Recientemente, el art. 27.3 del Reglamento de desarrollo de la LOPD se limita a afirmar que «[e]l derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común». Sobre la difícil conciliación entre la normativa de acceso a información administrativa y la de protección de datos personales, cfr. nuestro trabajo «Transparencia administrativa y protección de datos personales», cit., pp. 48-57. Cfr. sobre el derecho de acceso, S. FERNÁNDEZ RAMOS, *El derecho de acceso a los documentos administrativos*, Marcial Pons, Madrid, 1997; J. F. MESTRE DELGADO, *El derecho de acceso a archivos y registros administrativos. Análisis del art. 105.b) de la Constitución*, Madrid, 1998; E. GUICHOT, «Acceso a la información en poder de la Administración y protección de datos personales», *RAP*, nº 173, 2007, pp. 407-445.

de la LOPD es una de las facultades que integran el contenido esencial del derecho fundamental a la protección de datos personales y que permite el control de la propia información personal. Por ello, se trata de un acceso a los propios datos personales sometidos a tratamiento, no a datos de terceras personas y tiene tutela por una autoridad administrativa independiente. En cambio, el derecho de acceso de los ciudadanos del art. 105.b) de la CE es un acceso a los registros y a los documentos que formen parte de un expediente y obren en los archivos administrativos. No se solicitan los propios datos personales sometidos a tratamiento, sino una información administrativa, que, en muchas ocasiones, supone el acceso no sólo a datos propios sino a datos de terceras personas y permite la obtención de un expediente completo y la expedición de copias auténticas de cuantos documentos obraran en el mismo. Este derecho no dispone todavía en nuestro país de una tutela por una autoridad administrativa de control y se rige por la legislación administrativa –principalmente, por la LRJAP y PAC–. Así, el art. 35.a) de la LRJAP y PAC recoge el derecho de los ciudadanos a «a conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados, y obtener copias de documentos contenidos en ellos», mientras que el art. 37.1 de la LRJAP y PAC garantiza «el derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos […], siempre que tales expedientes correspondan a procedimientos terminados en la fecha de solicitud». Históricamente el derecho de acceso a archivos y registros administrativos previsto en la LRJAP y PAC se ejercitaba sobre una documentación administrativa que no siempre llevaba datos personales y, en el caso de que los llevara, no eran datos sometidos a tratamiento porque la información administrativa no se encontraba estructurada de conformidad con personas. Sin embargo, la implantación de la Administración electrónica hace que nos encontremos habitualmente dentro del ámbito de la LOPD que «será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento» –art. 2 LOPD–. Por ello, el ejercicio del derecho de acceso a archivos y registros administrativos que están en soportes automatizados tiene que respetar el ordenamiento jurídico de protección de datos personales(234). Así, en el supuesto de que la documentación administrativa en

(234) Así, la LOPD, a diferencia de la LORTAD, que excluía de su ámbito de aplicación «a los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general» [art. 2.2.a)], ha dejado claro que todos los registros administrativos se encuentran sometidos a la misma, sin perjuicio de que los ficheros del Registro Civil y del Registro Central de Penados y Rebeldes se rijan también por sus disposiciones específicas [art. 2.3.d)]. El art. 222.6 de la Ley Hipotecaria establece que los registradores, «al calificar el contenido de los asientos registrales, informarán y velarán por el cumplimiento de las normas aplicables sobre la protección de datos de carácter personal». Cfr. el Informe 2/2004 de la Agencia Española de Protección de Datos, accesible en su web, donde se señalan las competencias de control de la Agencia Española sobre estos ficheros y tratamientos del art. 2.3 de la LOPD.

soporte electrónico contenga información relativa a otras personas, estamos ante una cesión de datos personales, que puede hacerse sin consentimiento del interesado en virtud de una habilitación legal –art. 11.2.a) LOPD–, que en este caso sería la propia LRJAP y PAC(235). La LRJAP y PAC permite el acceso a datos nominativos por parte de terceras personas siempre que exista un interés legítimo y directo del art. 37.3 y prohíbe el acceso a datos referentes a la intimidad de la persona o a procedimientos sancionadores o disciplinarios, salvo al propio interesado. En todo caso, la regulación que lleva a cabo la LAECSP del derecho a conocer por medios electrónicos el estado de tramitación de un procedimiento y a obtener copias electrónicas de los documentos –art. 6.2.d) y e)– es diferente al derecho de acceso a los propios datos personales sometidos a tratamiento establecido en el art. 15 de la LOPD. Si bien no le corresponde a esta LAECSP regular el derecho de acceso del art. 15 de la LOPD, sí podía haber incluido expresamente dentro de los derechos de los ciudadanos del art. 6 la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición en el marco de la Administración electrónica.

Como hemos señalado antes, el derecho de acceso del art. 15 de la LOPD implica la posibilidad de solicitar y conocer los datos personales sometidos a tratamiento, el origen de dichos datos, las comunicaciones realizadas o que se prevén hacer en el futuro a terceras personas, a lo que añade el art. 27.2 del Reglamento de desarrollo de la LOPD la finalidad del tratamiento. El Reglamento de desarrollo de la LOPD permite que el objeto del derecho de acceso sea «la información disponible sobre el origen de los datos» –art. 27.2–. También las tecnologías de la información, en este caso aplicadas a la Administración electrónica, mejoran en este punto el control sobre la información personal, facilitando la traza del origen de los datos. Además, si bien no forma parte del contenido de este derecho la información sobre los diferentes accesos que se han producido en el fichero dentro del ámbito del responsable, sin embargo, parece razonable que el incremento del riesgo proveniente de la existencia de repositorios electrónicos de información personal –especialmente

(235) De hecho, una parte sustancial de los informes no preceptivos de las Agencias son sobre la adecuación o no de una cesión de datos personales. Así, el Tribunal de Primera Instancia, en su Sentencia de 8 de noviembre de 2007 –caso *Bavarian Lager*–, considera que el Reglamento 1049/2001 de Acceso a Documentos «constituye una obligación jurídica en el sentido del art. 5, letra b, del Reglamento 45/2001. En consecuencia, mientras que el Reglamento nº 1049/2001 obliga a la comunicación de datos, que constituye un tratamiento en el sentido del art. 2, letra b) del Reglamento nº 45/2002, el art. 5 de este Reglamento hace que tal comunicación sea lícita a este respecto» (párrafo 107). Sin embargo, la STS, de 25 de octubre de 2005, ha entendido que no hay afectación al derecho de protección de datos cuando se traslada un expediente a terceros interesados que son parte en un procedimiento administrativo, al entender que el derecho de acceso contemplado en el artículo 15 de la LOPD sólo opera cuando el tratamiento de los datos no lo sea en el marco de un procedimiento administrativo.

en el caso de datos especialmente protegidos como los que constan en historias clínicas electrónicas, en historias sociales electrónicas o en ficheros automatizados de orientaciones psicopedagógicas– sea compensado con medidas que impliquen un mayor reequilibrio como ofrecer al interesado información sobre el registro de los accesos a sus datos personales(236). Si el Reglamento de desarrollo de la LOPD señala que el ejercicio de los derechos de acceso, rectificación, cancelación y oposición debe poder realizarse a través de un medio sencillo y gratuito –entre los que incluye los servicios de atención al ciudadano o para la atención de reclamaciones (art. 24.2)–, los servicios de Administración electrónica facilitan el ejercicio de este derecho, lógicamente siempre que se garantice la identificación de la persona que lo ejercita –bien el propio interesado, bien alguien que actúa en su representación–, evitando accesos por terceras personas (237). En la medida de lo posible, el ejercicio del derecho de acceso deberá llevarse a cabo mediante la consulta directa por parte del interesado a través de los mismos medios electrónicos utilizados para el acceso al servicio electrónico de que se trate. El sistema deberá permitir al solicitante la elección del medio por el que desea recibir la información, promoviendo el uso de medios electrónicos seguros adecuados a la configuración o implantación material del fichero o a la naturaleza del tratamiento(238). Los medios electrónicos ayudan también al responsable a garantizar que el acceso del interesado es únicamente a sus datos personales sometidos a tratamiento y no se extiende a las apreciaciones subjetivas de los profesionales en el ámbito sanitario, social o en la atención psicopedagógica o a datos ofrecidos por terceras personas que están protegidos por el derecho a la intimidad. Si bien el art. 15.3 de la LOPD señala que el derecho de acceso «sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto», este límite temporal tenía sentido cuando el ejercicio del derecho suponía una carga de trabajo –y, por tanto, un coste– al responsable del fichero, pero lo pierde cuando este acceso a la

(236) Esta medida se está implementando en muchos modelos de historia clínica electrónica. Como hemos señalado en otro momento, la información contenida en el registro de accesos excede del art. 15 LOPD –porque no se trata en puridad de datos personales del interesado sometidos a tratamiento– y encajaría más con el derecho recogido en el art. 37 LRJAP y PAC.

(237) Los servicios de Administración electrónica deben exigir a las solicitudes de ejercicio de derechos todas las garantías que aseguren la identificación inequívoca del solicitante –sistemas de firma electrónica avanzada, incluyendo los incorporados al Documento Nacional de Identidad, u otros medios, como la introducción de una clave de acceso personalizada previamente asignada por la Administración, con su correspondiente contraseña, la aportación de información sólo conocida por ambas partes, o mecanismos equivalentes–. Es especialmente importante la identificación cuando se accede a datos especialmente protegidos. Es necesario proceder a la identificación de padres o tutores, por ejemplo, cuando se emplean medios electrónicos para ofrecer información sobre calificaciones y otras incidencias de los menores en el ámbito educativo.

(238) Sobre esta cuestión, cfr. la Recomendación 3/2008 de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica.

propia información personal puede hacerse *on line* por el interesado a través de los servicios de Administración Electrónica. La utilización de medios electrónicos para el acceso a los datos personales debe servir también para acortar los plazos para el cumplimiento de este derecho por parte del responsable del fichero, algo especialmente importante cuando se emplea como instrumento de garantía para el ejercicio de otros derechos fundamentales. Éste sería el caso del acceso del paciente a su historia clínica y a una copia de la misma por medios electrónicos, que tiene que ser rápida para permitir la libertad y autonomía del paciente para el cambio de centro hospitalario o de facultativo o para pedir otra opinión clínica. Los servicios de Administración electrónica tienen que permitir el ejercicio del derecho de oposición –art. 6.4 LOPD–, rectificación y cancelación –art. 16 LOPD–. Al igual que ocurría con el derecho de acceso a los propios datos personales sometidos a tratamiento del art. 15 de la LOPD, que era distinto al derecho a conocer por medios electrónicos el estado de tramitación de un procedimiento y a obtener copias electrónicas de los documentos, también el derecho de rectificación y cancelación del art. 16 LOPD es distinto de la facultad del interesado de rectificar los errores materiales, de hecho o aritméticos en los actos administrativos –arts. 37.2, 105.2 y 118 LRJAP y PAC–(239). Es importante, como hemos señalado en otro momento, que cuando un ciudadano ejerza el derecho de rectificación se corrija también la información que se haya comunicado a otras Administraciones Públicas, para lo que es necesario que exista un rastro en los distintos accesos e interconexiones entre bases de datos de las Administraciones Públicas. Lógicamente, cuando no exista este modelo de interconexión y en garantía de que no hay cesiones sin consentimiento del interesado o habilitación legal, cuando un ciudadano ejerce el derecho de rectificación tiene que hacerlo en cada uno de los Entes públicos a los que ha dado sus datos. Los medios electrónicos, además de servir también para agilizar la rectificación de datos erróneos o inexactos –que pueden perjudicar el ejercicio de otros derechos o la percepción de prestaciones sociales–, permitiendo que la información responda con veracidad a la situación actual del afectado, favorecen el bloqueo de los datos de forma que sólo accedan a la información aquellas personas que deban atender las posibles responsabilidades. En la actualidad, el derecho de consulta al registro general de protección de datos y a los registros autonómicos se puede llevar a cabo por medios electrónicos –art. 14 LOPD–.

Hay que recordar la especial vigencia que tiene en el ámbito de la Administración electrónica el derecho de los ciudadanos «a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte

(239) Como señala el art. 25 del Reglamento de desarrollo de la LOPD, cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas –art. 25.8–.

de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad» –art. 13.1 LOPD–(240). Este derecho supone un importante límite para las decisiones administrativas adoptadas únicamente en virtud de un cruce de bases de datos. Este derecho atribuye al ciudadano la posibilidad de impugnar actos administrativos «que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad» –art. 13.2–. Si bien las decisiones administrativas no se encuentran basadas en la personalidad, sí lo pueden estar en virtud de las características personales. El Reglamento de desarrollo de la LOPD permite las decisiones administrativas que se basen únicamente en un tratamiento automatizado de datos destinados a evaluar determinados aspectos de la personalidad cuando estén autorizadas por una norma de rango legal que establezca medidas que garanticen el interés legítimo del interesado –art. 36.2.b)–(241). Hay que resaltar que el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto –art. 13.3 LOPD–(242). Hay que mencionar que la LAECSP prevé la utilización de medios electrónicos en la tramitación del procedimiento administrativo –arts. 35-39– y establece la existencia de actuaciones administrativas automatizadas que son producidas por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Esta actuación administrativa automatizada incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación –Anexo a)–(243). Como única garantía se

(240) El Reglamento de desarrollo de la LOPD, al igual que la Directiva 95/46/CE, regula de manera conjunta dentro del derecho de oposición el de impugnación de valoraciones (art. 34).

(241) El Reglamento de desarrollo de la LOPD también señala en el art. 36.2.a) que el afectado tendrá que aceptar la decisión basada sólo en tratamientos automatizados cuando se ha adoptado en el marco de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estime pertinente. Pero el responsable «deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas». El derecho a la impugnación de valoraciones se puede ejercitar, por ejemplo, en el ámbito de los servicios sociales, donde la cantidad concreta con la que debe contribuir el usuario a financiar la prestación de un servicio social –o su gratuidad– se determina en función de un programa informático alimentado con los datos recabados de los interesados que no siempre disponen de información relativa a la fórmula matemática que sirve para dar el resultado final.

(242) «La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado» –art. 13.3 y 4 LOPD–.

(243) El art. 96.3 y 4 de la Ley 58/2003, de 17 de diciembre, General Tributaria, señala «los procedimientos y actuaciones en los que se utilicen técnicas y medios electrónicos, informáticos y telemáticos garantizarán la identificación de la Administración tributaria actuante y el ejercicio de su competencia. Además, cuando la Administración tributaria actúe de forma automatizada se garantizará la identificación de los órganos competentes para la programación y supervisión del sistema de información y de los órganos competentes para resolver los

indica que «deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación» –art. 39–. Lógicamente, a nuestro juicio, también podrá exigirse información del responsable sobre el programa utilizado en el tratamiento que sirvió para la decisión administrativa.

Corresponde a la Agencia Española de Protección de Datos y a las Agencias Autonómicas velar por el cumplimiento de la legislación de protección de datos y controlar su aplicación, garantizando los principios y derechos de protección de datos personales, también en el ámbito de la Administración electrónica –arts. 37 y 41 LOPD–(244). Sin embargo, la LAECSP crea la figura del defensor del usuario de la Administración electrónica que «velará por la garantía de los derechos reconocidos a los ciudadanos en la presente Ley, sin perjuicio de las competencias atribuidas en este ámbito a otros órganos o entidades de derecho público» –art. 7.1–. Como esta Ley menciona entre los derechos de los ciudadanos frente a la Administración electrónica la garantía de la seguridad y confidencialidad de los datos que figuren en ficheros, sistemas y aplicaciones de las Administraciones Públicas –art. 6.2.i)–, las competencias de este defensor del usuario afectarían a las Agencias de Protección de Datos, especialmente a las competencias de la Agencia Española de Protección de Datos. Hay que señalar que el defensor del usuario, si bien desarrolla

---

recursos que puedan interponerse». Los programas y aplicaciones electrónicas, informáticas y telemáticas que vayan a ser utilizados por la Administración tributaria para el ejercicio de sus potestades habrán de ser previamente aprobados por ésta en la forma que se determine reglamentariamente. Igualmente establece en el art. 100.2 que «[t]endrá la consideración de resolución la contestación efectuada de forma automatizada por la Administración tributaria en aquellos procedimientos en que esté prevista esta forma de terminación».

(244) El incremento de las comunicaciones de datos personales entre Administraciones Públicas derivado de la implantación de la Administración electrónica no afecta a las competencias de las Agencias de Protección de Datos, que están delimitadas en virtud de quién sea el responsable del fichero o del tratamiento. Cfr. nuestro trabajo «Las Comunidades Autónomas y la protección de datos personales a la luz de las reformas estatutarias», en *Estudios sobre Comunidades Autónomas y Protección de Datos Personales*, Civitas-APDCM, Madrid, 2006 pp. 19-138. En España no es posible ir hacia un modelo centralizado de ficheros, dada la distribución constitucional de competencias. Así, no existirá un fichero centralizado de historias clínicas sino un sistema de información sanitaria básica del ciudadano que lidera el Ministerio de Sanidad y que comparten los Servicios de Salud de las Comunidades Autónomas que son responsables de los ficheros de historia clínica electrónica en cada uno de sus territorios. Por tanto, el intercambio de información es consecuencia del modelo constitucional descentralizado, que no sólo afecta a la titularidad de los ficheros sino a la propia existencia de autoridades de control en algunas CC AA. Habrá un modelo de fichero centralizado con múltiples accesos para consultar la información cuando la competencia administrativa se encuentre centralizada –como es el caso de los DIN–, un fichero centralizado con accesos de las diferentes Administraciones Públicas para la verificación de datos de identidad.

sus funciones «con imparcialidad e independencia funcional», no tiene el carácter de Administración independiente, entre otras razones, porque no dispone de la garantía de inamovilidad(245). Tanto la Directiva 95/46/CE y la Carta de Derechos Fundamentales de la Unión Europea como la LOPD exigen que la tutela de los derechos de las personas frente a los tratamientos de sus datos personales recaiga en una autoridad independiente(246) por lo que la actividad del defensor del usuario no puede mermar las competencias de las Agencias de Protección de Datos que se configuran como entes de derecho público con plena independencia de las Administraciones Públicas para velar por el cumplimiento de la legislación sobre protección de datos –arts. 35 y 37.a) LOPD–. Igualmente, la existencia de Administraciones Públicas que sancionan conductas en relación con la Administración electrónica –por ejemplo, la competencia del Ministerio de Ciencia y Tecnología y de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información para la imposición de sanciones por incumplimiento de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, ambos órganos dependientes del poder ejecutivo– tampoco limita en este ámbito la actividad de las Agencias de Protección de Datos Personales de control y tutela de este derecho fundamental. Así, la LOPD tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar. Por tanto, todos los tratamientos de datos personales son objeto del derecho fundamental a la protección de datos personales y todos están sometidos a una autoridad de control independiente. No es posible que existan tratamientos de datos personales excluidos del objeto del derecho fundamental –salvo aquellos específicamente mencionados en el art. 2.2 LOPD– o no sometidos al control de una autoridad independiente. Por ello, todos los responsables de los ficheros y los encargados de los tratamientos de datos personales están sujetos al régimen sancionador establecido en la LOPD –art. 43.1–(247) y están

(245) La figura del defensor del usuario es estudiada por COTINO, que considera su regulación poco sólida, con una excesiva dependencia de medios de la Inspección de Servicios y con nulas garantías de independencia en cuanto a su nombramiento y cese. Cfr. L. COTINO HUESO, «Los derechos del ciudadano», cit., pp. 221-224.

(246) Cfr. A. TRONCOSO REIGADA, «Las Agencias de Protección de Datos como Administración independiente», en C. PAUNER CHULVI y B. S. TOMÁS MALLÉN, *Las Administraciones independientes*, Tirant lo Blanch, Valencia, 2009, pp. 27-216.

(247) La Agencia de Protección de Datos de Madrid, en la Resolución de 29 de julio de 2009, declaró a la Dirección General de Movilidad del Ayuntamiento de Madrid varias infracciones a la legislación de protección de datos personales por vulneración de los arts. 4 y 12 de la LOPD en la recogida de datos para la atribución de la firma electrónica de los empleados. Lógicamente, en la determinación de las posibles infracciones –por ejemplo para la determinación del cumplimiento del principio de calidad que prohíbe los tratamientos excesivos– se acude a la legislación sectorial –en este caso a la Ley de 59/2003, de 19 de diciembre como en otras ocasiones a la legislación administrativa o a la de autonomía del paciente–, pero esto no excluye a estos tratamientos de datos personales de la protección de este derecho fundamental. Por tanto, la Ley 59/2003, de 19 de diciembre, de firma electrónica podrá servir para inter-

obligados a indemnizar cuando los ciudadanos sufran daño o lesión en sus bienes o derechos por el funcionamiento de los servicios de Administración electrónica –art. 19.2 LOPD–.

---

pretar los principios de protección de datos –en este caso, el principio de calidad–, pero no puede exceptuar la actividad de la Autoridad de Control en materia de protección de datos. De hecho, la propia Ley 59/2003, de 19 de diciembre lo asume expresamente cuando afirma que el tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esa Ley se sujetará a lo dispuesto en la LOPD –art. 17.1–. La Ley 59/2003, de 19 de diciembre, establece como objeto de la misma regular la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación –art. 1–, atribuyendo al Ministro de Ciencia y Tecnología y al Secretario de Estado de Telecomunicaciones la imposición de sanciones por incumplimiento de la Ley, ambos órganos dependientes del poder ejecutivo. No hay, por tanto, ningún *bis in idem* posible ya que la infracción de protección de datos lesiona un bien jurídico distinto a las infracciones a la ley de firma electrónica. De hecho, hay que diferenciar la responsabilidad de la Dirección General de Movilidad del Ayuntamiento de Madrid, como responsable de la recogida de datos personales de empleados para la gestión del certificado de la firma digital, de la eventual responsabilidad de la Fábrica Nacional de Moneda y Timbre, como prestador de servicios de certificación, un procedimiento de infracción que en su caso deberá seguir el Ministerio de Ciencia y Tecnología y la Secretaría de Estado de Telecomunicaciones, al amparo de lo dispuesto en la Ley 59/2003, de 19 de diciembre.