LA ADMINISTRACIÓN ELECTRÓNICA Y LA PROTECCIÓN DE DATOS PERSONALES

Antonio Troncoso Reigada
Profesor Titular de Derecho Constitucional
Director de la Agencia de Protección de Datos de la Comunidad de Madrid

Las nuevas tecnologías son un importante instrumento para la modernización de las Administraciones Públicas que permiten a éstas ser más eficaces en el servicio al interés general y en la promoción de los derechos fundamentales. De entre las distintas iniciativas hay que destacar especialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que consagra el derecho de éstos a comunicarse con las Administraciones por medios electrónicos. Lógicamente, esto supone un incremento de los tratamientos de datos personales por las Administraciones Públicas, que deben respetar en todo caso el derecho fundamental a la protección de datos personales. Es especialmente importante el respeto a este derecho fundamental en las interconexiones de bases de datos de Administraciones Públicas, ya que éstas incrementan el riesgo y suponen una mayor injerencia en el derecho fundamental a la protección de datos personales. Es necesario que estas interconexiones respeten el principio de proporcionalidad, lo que 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—. Además, es necesario que se respeten los supuestos que legitiman la cesión —que exista consentimiento

del interesado, una habilitación legal, que la comunicación sea necesaria para verificar la exactitud de datos facilitados por el ciudadano que estén en poder de las Administraciones Públicas, que exista una relación negocial o que sea para competencias semejantes sobre materias comunes—. Es muy importante respetar el principio de calidad y de finalidad de forma que la transmisión de datos entre Administraciones Públicas esté limitada estrictamente a aquellos datos necesarios para la resolución del procedimiento administrativo. También hay que resaltar la obligación de informar al ciudadano sobre las cesiones de datos entre Administraciones Públicas, especialmente cuando estas cesiones se realizan sin su consentimiento de forma que pueda de alguna manera controlar el uso de su información personal. Si bien no hace falta el consentimiento para el tratamiento de datos personales para el cumplimiento de funciones Administrativas —lo que permite los tratamientos automatizados—, la Administración no puede imponer a los ciudadanos que se relacionen con ella a través de medios electrónicos. Además, es necesario el consentimiento del interesado cuando la Administración Pública recoge datos personales para ofrecer determinados servicios como los de noticias y alertas o para la introducción de cookies *para dar un valor añadido, ya que éstas no son funciones administratrivas. También es muy importante la seguridad de la información en el ámbito de la Administración electrónica, puesto que la autenticidad y la integridad de los datos personales y de los documentos administrativos es imprescindible para la tutela de los derechos y para el normal funcionamiento de la actividad administrativa. La Administración electrónica debe facilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, especialmente del derecho de impugnación de aquellas decisiones administrativas adoptadas únicamente en virtud de un cruce de bases de datos. En todo caso, la voluntad de mejorar la protección de los datos personales en la Administración electrónica aconseja alcanzar algunas sinergias con la industria de las TIC, que ayude a construir las denominadas «tecnologías de protección del derecho a la intimidad (PET)».*

SUMARIO

1. LAS NUEVAS TECNOLOGÍAS COMO INSTRUMENTO DE MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS: LA ADMINISTRACIÓN ELECTRÓNICA.

2. DE LA TEORÍA DE LA ADMINISTRACIÓN ELECTRÓNICA A LA REALIDAD: INICIATIVAS Y OBSTÁCULOS. LA LEY 11/2007, DE 22 DE JUNIO, DE ACCESO ELECTRÓNICO DE LOS CIUDADANOS A LOS SERVICIOS PÚBLICOS.

3. LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA.

   3.1. El incremento de los tratamientos de datos personales en la Administración electrónica. Las tecnologías de protección del derecho a la intimidad.

   3.2. El principio de calidad. La finalidad del DNI electrónico y los datos objeto de tratamiento.

   3.3. La información y el consentimiento. Servicios de noticias y alertas y uso de *cookies*.

   3.4. Los accesos electrónicos, las interconexiones y el respeto al principio de proporcionalidad.

   3.5. La seguridad como garantía de la integridad, autenticidad y confidencialidad de la información administrativa.

   3.6. El ejercicio de los derechos y la actividad de las autoridades de control.

1. LAS NUEVAS TECNOLOGÍAS COMO INSTRUMENTO DE MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS: LA ADMINISTRACIÓN ELECTRÓNICA

Las nuevas tecnologías de la información y la comunicación —especialmente Internet— han revolucionado la vida y las relaciones comerciales. La introducción de las nuevas tecnologías de la información y la comunicación afecta tanto a la sociedad como a la Administración. Internet no es el futuro: es ya el presente y está aquí para quedarse. Los poderes públicos están desarrollando por ello un conjunto de estrategias de administración electrónica para prestar servicios públicos y facilitar la participación social. El desarrollo de estas nuevas tecnologías en la Administración y, en especial, los proyectos de gobierno electrónico tienen que comprenderse y analizarse dentro de las iniciativas que tratan de mejorar la calidad de los servicios públicos y de modernizar la Administración Pública [(1)]. La aplicación de las tecnologías de la información supone una revolución interna en la Administración Pública y es una importante herramienta para la consecución de una mayor modernización administrativa. Es, por tanto, ne-

---

1. Cfr. E. DEL PINO: *Los ciudadanos y el Estado. Las actitudes de los españoles hacia las Administraciones y las políticas públicas*, INAP, 2004; *Reflexiones para la modernización de la Administración del Estado*, MAP, 1990; *La Modernización de la Administración del Estado. Los Servicios Comunes*, Jornadas para la Modernización de las Administraciones Públicas, 9, 10 y 11 de julio de 1990, Cuenca, MAP, 1991; A. MUÑOZ MACHADO: *La Gestión de la Calidad Total en la Administración Pública*, Díez de Santos, 1999; *Libro Blanco para la Mejora de los Servicios Públicos*: «*Una nueva Administración al servicio de los ciudadanos*», MAP, 2000. Cfr. también J.J. FERNÁNDEZ RODRÍGUEZ: *Gobierno Electrónico. Un desafío en Internet*, FUNDAP, 2004; L. COTINO HUESO (coord.), *Libertades, democracia y gobierno electrónicos*, Comares, Granada, 2005. Han existido un conjunto de proyectos concretos que es bueno destacar. Cfr. *Plan Estratégico para la Calidad en el Gobierno de La Rioja*, Gobierno de La Rioja. Consejería de Desarrollo Autonómico y Administraciones Públicas, 2000; *El proceso de la modernización en las Administraciones Públicas. El caso de La Rioja*, Gobierno de La Rioja. Consejería de Desarrollo Autonómico y Administraciones Públicas, 2000; *Plan Marco de Modernización 2005/2007*, Gobierno de Cantabria, 2006; *Libro Blanco para la Innovación y la Mejora de los Servicios Públicos del Gobierno de Cantabria*, Consejería de Presidencia, 2003; *Modernización en el Ayuntamiento de Madrid*, Ayuntamiento de Madrid, 2005; *Alcobendas, ¡qué diferencia! Balance Plan Ciudad Ayuntamiento de Alcobendas*, 2003.

cesario reflexionar acerca de las políticas de reforma de la Administración pública, para analizar dónde estamos —qué hemos hecho hasta ahora— y a dónde queremos llegar —qué modelo de Administración tenemos—.

Desde los años 90, los Gobiernos están desarrollando un proceso de modernización que tiene como objetivos preferentes: por una parte, acercar la Administración a los ciudadanos; por otra, mejorar la satisfacción de éstos en relación con los servicios que les presta la Administración Pública. Se pretende con ello que la Administración se ajuste a los principios constitucionales de eficacia y de servicio al interés general. Las Administraciones Públicas desarrollan distintas actividades y prestan servicios públicos. Los ciudadanos exigen de la Administración cada vez mejores servicios públicos, no solo en virtud de los impuestos que pagan, sino porque como ciudadanos son titulares de unos derechos fundamentales que la Administración Pública debe respetar y promover. En este marco se encuadran los distintos Decálogos de Derechos de los Ciudadanos frente a la Administración Pública, 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 figuras como la del Defensor del Contribuyente como órgano de tutela de los ciudadanos en sus relaciones con la Administración tributaria [(2)].

La introducción de las nuevas tecnologías debe enmarcarse en este contexto de modernización administrativa [(3)]. Las nuevas tecnologías no son un fin en sí mis-

---

2. Cfr. más ampliamente 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. Cfr. también 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*, núm. 40, 2000.

3. La mayoría de los proyectos de modernización administrativa han sido liderados en nuestro país por la Comunidad de Madrid, que fue la primera Administración Pública que puso en marcha una Dirección General de Calidad de los Servicios. Hay que reconocer especialmente el trabajo de J.L. Moreno Casas, primer Director de Calidad de los Servicios en los Gobiernos de Ruiz Gallardón, auténtico pionero en este campo. También tuve la oportunidad de continuar esos proyectos sucediéndole como Director General de Calidad en los Gobiernos de Ruiz Gallardón. De entre las publicaciones de la Comunidad de Madrid desde los años 1995-2000 puedo destacar*: En busca de la Excelencia: El modelo EFQM de excelencia en la Administración de la Comunidad de Madrid*; *Memoria de los Premios a la Excelencia y Calidad del Servicio Público; Diez veces 10. Ejemplos de Prácticas de Calidad en la Comunidad de Madrid*, 1998*; Calidad.com, Ejemplos de Prácticas de Calidad en la Comunidad de Madrid; Cuadro de Indicadores de Calidad de la Comunidad de Madrid; Medir para Mejorar;*

mo, sino una herramienta de cambio y de modernización administrativa que contribuye a acercar la Administración a los ciudadanos y, en definitiva, a mejorar la satisfacción de éstos por los servicios públicos que reciben (4). Las nuevas tecnologías facilitan un nuevo cauce de relación entre la Administración y los ciudadanos, de manera que esta relación 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, al poderse desarrollar en todas las horas y desde el propio domicilio o lugar de trabajo (5). Además, las nuevas tecnologías no deben servir sólo para mejorar la información que las Administraciones Públicas dan a los ciudadanos sino también para permitir la tramitación telemática 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 (6) o conocer el estado de tramitación de un expediente administrativo.

Observatorio de la Calidad 1998-2002. Indicadores de Calidad de las Áreas de Información y Atención al Ciudadano; 150 Proyectos de Mejora de la Calidad en la Comunidad de Madrid. Cfr. también M. SALVADOR SERNA*: La configuración del sistema de función pública de la Comunidad de Madrid. Instituciones y políticas públicas en la gestión de recursos humanos de la Administración de la C.M.*, IMAP, 2006.

4. 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)*».*

5. 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»* —apartado I—.

6. Sobre esta cuestión nos hemos referido en el Prólogo del *Manual de Protección de Datos Personales para las Administraciones Públicas*, Civitas, Madrid, 2004.

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 a la automatización del *back office* administrativo, es decir, a la mecanización de los procedimientos. Ahora bien, antes que automatizar los procedimientos, hay que rediseñarlos. De esta forma, la Administración electrónica lleva aparejado el impulso de los procesos de simplificación administrativa (7). Esto significa 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 (8)—, implantar bases generales de procedimientos y plazos únicos y la instauración progresiva del silencio positivo como regla general (9). Todo ello permite una gestión administrativa más rápida y más clara.

El desarrollo de la Administración electrónica permite dar una más extensa información administrativa sobre concursos, contratos, subvenciones, procesos selectivos, no sólo a ciudadanos en concreto sino a asociaciones y a la sociedad en general; esta información, en ocasiones, sólo la tenían funcionarios y grupos de interés. De esta forma, la Administración electrónica mejora la posición de los ciudadanos frente a la Administración Pública y asegura la transparencia administrativa y el control social sobre ella (10), una cuestión que abordaremos más adelante.

---

7. 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 Simplificación Administrativa elaborado por la Comunidad de Madrid en el año 2000 durante mi etapa como Director General.

8. No se le puede exigir a un ciudadano para la solicitud de una subvención estar al día de las obligaciones tributarias o con la Tesorería de la Seguridad Social si esta información la puede solicitar directamente el órgano administrativo a otra Administración, a través de interconexiones de bases de datos con los necesarios convenios interadministrativos. Se materializa así un derecho de los ciudadanos de no tener que aportar documentación que ya tenga la Administración. Cfr. artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común —hoy ya parcialmente derogado— y Real Decreto 263/1996, de 16 de febrero, que desarrolla este artículo. A esta cuestión nos referiremos posteriormente.

9. El silencio positivo obliga a la Administración a resolver expresamente y en plazo y a justificar la resolución.

10. 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

La Administración electrónica también permite mejorar la participación de los usuarios en el diseño y gestión de los servicios públicos (11). De hecho, la mejora 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 mejor, la que permite aprovechar mejor los fondos públicos es siempre aquélla 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 (12). Los medios electrónicos permiten una Administración más democrática.

---

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 pagina 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*, núm. 32, 1999, p. 8.

11. 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*, junio de 2004.

12. 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 deben ser abordados en otro momento. 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. Cfr. *Democracia electrónica y participación ciudadana. Informe tecnológico y funcional sobre la Consulta Ciudadana*, «Madrid Participa», julio de 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 del Bies 35 tiene canales electrónicos aunque los accionistas prefieren todavía el correo postal a la hora de remitir sus votos a distancia. Cfr. *Cinco días*, jueves, 4 de agosto de 2005.

La Administración electrónica 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 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. Los ciudadanos cada vez piden más prestaciones, exigen más de la Administración. La mejora de la calidad de los servicios públicos y el incremento de las ayudas sociales pueden venir gracias al ahorro de recursos que supone la Administración electrónica. 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 [13]; la historia clínica electrónica evita la repetición de pruebas diagnósticas y mejora la calidad asistencial, especialmente de los pacientes desplazados [14]. La informatización y la automatización de procedimientos reducen también 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 tienen que 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 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

13. 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.

14. Cfr. nuestra Introducción a *Protección de datos personales para Servicios Sanitarios Públicos,* Civitas-APDCM, Madrid, 2008.

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 [15].

Por tanto, se puede concluir que las nuevas tecnologías suponen un instrumento de modernización y cambio en las Administraciones Públicas. En el ámbito de la Administración pública, las nuevas tecnologías, especialmente Internet, contribuyen a mejorar la actividad administrativa en beneficio del interés general y a actuar de conformidad con el principio de eficacia. Si bien las Administraciones Públicas tienen 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 [16] y con el respeto al principio de eficacia [17]. Por ello, la Administración electrónica también mejora la legitimidad de los poderes públicos.

2. DE LA TEORÍA DE LA ADMINISTRACIÓN ELECTRÓNICA A LA REALIDAD: INICIATIVAS Y OBSTÁCULOS. LA LEY 11/2007, DE 22 DE JUNIO, DE ACCESO ELECTRÓNICO DE LOS CIUDADANOS A LOS SERVICIOS PÚBLICOS

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común asumió que la adaptación a las nuevas tecnologías debía ser una característica permanen-

---

15. Cfr. nuestra introducción a la *Memoria del I Premio Europeo de Mejores Prácticas de las Administraciones Públicas en Protección de Datos Personales*, Civitas, Madrid, 2005.

16. Cfr. *Satisfacción de los Ciudadanos y Ciudadanas en la Comunidad de Madrid*, 1999.

17. Cfr. A. VALARIE, A. ZEITHAML, L. BERRY: *Calidad total en la gestión de servicios*. Delivering Quality Service, Díaz de Santos, 1992; *Guía para la implantación de sistemas de indicadores. Norma UNE 66175*, AENOR, 2006; *Evaluando servicios y políticas públicas,* Gobierno de Cantabria, Consejería de Presidencia, 2006; *Gestión y Evaluación de la Calidad en los Servicios Públicos*. Segundas Jornadas sobre Medición y Mejora de los Servicios Públicos, MAP, 1995; *Guía para la Gestión de la Calidad de los Servicios Públicos* (Adaptación de la Norma UNE-EN-ISO 9004-2), Ministerio de Administraciones Públicas, Consejería de Economía y Hacienda del Gobierno de Canarias y Asociación Española para la Calidad, 2000.

te de las Administraciones Públicas españolas [18]. Por ello 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. Así, el artículo 45.1 y 2 de la Ley 30/1992, de 26 de noviembre, indica que *«[l]as Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las Leyes. Cuando sea compatible con los medios técnicos de que dispongan las Administraciones Públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos y telemáticos con respeto de las garantías y requisitos previstos en cada procedimiento».* El artículo 38.3 afirma que *«[l]os registros generales así como todos los registros que las Administraciones Públicas establezcan para la recepción de escritos y comunicaciones de los particulares o de órganos administrativos deberán instalarse en soporte informático».* También se prevé la existencia de notificaciones por medios telemáticos —artículo 59.3—. Igualmente, la Ley 30/1992, de 26 de noviembre trata de modernizar la gestión de la Administración Pública, simplificando la necesidad de aportar documentos que se encuentren ya en poder de la Administración. Así, reconoce el derecho de los ciudadanos en sus relaciones con las Administraciones Públicas *«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»* —artículo 35.f)—. Es necesario mencionar 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, incorporando un nuevo apartado noveno al artículo 38 relativo a los registros telemáticos y un apartado tercero al artículo 59 relativo a las notificaciones telemáticas [19]. El Real

18. Cfr. como referencia general J. VALERO TORRIJOS, *El régimen jurídico de la e-Administración*, Comares, Granada, 2004. En todo caso 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 automoción 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* núm. 3, 2007, p. 103.

19. Esta Ley introduce una nueva Disposición Adicional Decimoctava en la LRJAP y PAC que obliga a determinadas empresas y personas físicas a presentar sus solicitudes y comunicaciones a las Administraciones Pú-

Decreto 263/1996, de 16 de febrero efectúa una regulación de las técnicas electrónicas, informáticas y telemáticas en el ámbito de la Administración del Estado para proporcionar la validez jurídica necesaria para que estos sistemas de información puedan ser realmente utilizados para el ejercicio de competencias atribuidas a los órganos administrativos [20]. En todo caso, hay que señalar que la existencia de una Administración electrónica no era una obligación sino una posibilidad de la distintas Administraciones Públicas.

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—. Uno de los principales objetivos de e-Europe era la modernización de los servicios públicos, mediante la puesta en marcha de la Administración electrónica. Se pretendía poner a las Administraciones Públicas en línea. Así se buscaba: la conexión de banda ancha para Administraciones públicas antes de 2005 —especialmente centros escolares y centros de salud—; la provisión de servicios públicos interactivos —antes de finalizar 2004—; la realización por medios electrónicos de una parte significativa de la contratación pública de los Estados miembros —antes de finalizar el 2005—; la prestación de servicios sanitarios en línea —esto ya estaba en el e-Europe 2000 para antes del 2002, lo que implicaba tarjeta sanitaria, redes de información sanitaria—; el aprendizaje en línea, a través de centros escolares conectados a internet, programas en *e-learning*, campus virtuales para todos los estudiantes; puntos de acceso públicos a internet, con conexiones en banda ancha, preferiblemente en los municipios; mejora de la seguridad, con autenticación electrónica y tarjeta inteligente; y acceso de personas con discapacidades a las páginas web

---

blicas mediante medios telemáticos, cuando así lo establezca una Orden del departamento ministerial correspondiente.

20. Este Real Decreto ha sido modificado por el Real Decreto 209/2003, de 21 de febrero, que aborda las notificaciones telemáticas. Hay que mencionar también el Real Decreto 772/1999, de 7 de mayo, que regula la presentación de escritos y solicitudes ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro. Este Real Decreto facilita el establecimiento de modelos normalizados de escritos y solicitudes que, además, permitan su transmisión por medios telemáticos. En la Comunidad de Madrid se aprobó el Decreto 175/2002, de 14 de noviembre, por el que se regula la utilización de las técnicas electrónicas, informáticas y telemáticas por la Administración de la Comunidad de Madrid.

públicas —e-Europe 2002— [21]. El sector de las finanzas públicas es un ámbito de intervención privilegiada de la Administración electrónica ya que casi todos los países europeos ofrecen la posibilidad de recurrir a un procedimiento de declaración del impuesto sobre la renta en línea en línea [22].

Una de las primeras iniciativas del Gobierno español para el fomento de la sociedad de la información se denominó Proyecto INFO XXI. Si bien algunos de los programas no obtuvieron los resultados esperados, sí existieron distintas iniciativas de éxito, especialmente en el ámbito de la Administración electrónica. Así, la Agencia Estatal de Administración Tributaria es líder mundial en el pago de impuestos por internet. En nuestro país se permite el pago de impuestos *on line* desde 1999, habiéndose presentado 2.500.000 declaraciones de IRPF *on line* en el año 2005 [23]. Por ello, la Agencia Estatal de Administración Tributaria fue seleccionada *best practice* a nivel europeo en Administración Electrónica. Igualmente España ha sido el primer país del mundo que ha permitido a sus ciudadanos cumplimentar el censo íntegramente por internet —algo que sólo habían logrado de forma parcial Suiza y Singapur—. También existe un notable desarrollo de la gestión del IVA y de los trámites con la Seguridad Social, mediante el sistema RED en internet. La Fábrica Nacional de

---

21. 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. Recientemente se ha aprobado 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 es una continuación de los anteriores.

22. El Grupo de Trabajo del Artículo 29 también destaca otros procedimientos como la notificación administrativa de cambio de dirección o el procedimiento en línea de búsqueda de empleo. *«Los países europeos también resaltan otros procedimientos en línea como las solicitudes de permisos de obras, los préstamos en bibliotecas públicas, la solicitud de documentos al registro civil, los procedimientos de registro de nuevas empresas, las cargas sociales, las relaciones de los usuarios con los profesionales de los centros sanitarios, la matrícula en escuelas y universidades, las inscripciones en exámenes, la matriculación de coches, el reembolso de gastos médicos y, por último, el registro de demandas (policía, justicia, etc.), éste último asociado, en general, a un servicio de envíos por correo»*. Cfr. el documento del Grupo de Protección de datos del artículo 29, relativo a la administración en línea, adoptado el 8 de mayo de 2003. 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, en <http://www.europa.eu.int/comm/privacy>.

23. El incremento fue progresivo: 20.000, 120.000, 500.000, 1.700.000 y 2.326.000.

Moneda y Timbre a través de CERES ha desarrollado un completo sistema de certificación electrónica, habiendo emitido en mayo de 2005 más de 700.000 ciudadanos —muchos de ellos, de gestorías—.

La Comisión Europea ha señalado a España como líder en algunos servicios de Administración electrónica, siendo el quinto país de la Unión europea en implantación [24]. El nivel de penetración de la sociedad de la información en España es mayor en la Administración Pública y menor en la sociedad. Nuestro país todavía se encuentra en una situación de desventaja en Europa y en la OCDE en cuanto a índices de desarrollo de la sociedad de la información, posición que no se corresponde con nuestra situación económica ni con los índices de convergencia con las economías de nuestro entorno comunitario. Esta situación fue analizada por la denominada *«Comisión Soto»*. Los planteamientos elaborados por esta Comisión fueron llevados a la iniciativa España.es [25], sucesora del plan inicial INFO XXI, y que incluye un apartado denominado *«administración.es»* [26]. El desarrollo de la Administración electrónica era, para la Comisión Soto, una de las medidas fundamentales para el desarrollo de la sociedad de la información. Era 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. La Comisión Soto apostó por una utilización generalizada de las nuevas tecnologías en las Administraciones Públicas tanto en la relación con los ciudadanos como en lo relativo a la informatización de los procedimientos internos. De esta forma, la Administración electrónica no es solo una oportunidad histórica para avanzar hacia un mejor gobierno del Estado, aumentando la eficiencia y ofreciendo un mejor servicio al ciudadano. Asimismo, 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.

---

24. Informe de la Comisión europea y CapGemini Ernst & Young, octubre de 2002.

25. <http://www.red.es/MungoBlobs/espana_es.pdf>.

26. <http://www.setsi.mcyt.es/espana_es/espana_es.htm>. Este proyecto fue presentado el 8 de mayo de 2003 por el Ministerio de Ciencia y Tecnología y por el Ministerio de Administraciones Públicas, apoyado a través de la Entidad Pública Empresaria Red.es.

El proyecto administracion.es trataba principalmente de superar un enfoque departamental para ir a un modelo centrado en el usuario. Se pretendía configurar un punto de acceso único a los servicios de administración electrónica, que albergase un número elevado de servicios —una oferta integrada de servicios—, sin perjuicio de que los ciudadanos sigan accediendo a los servicios que les ofrecen los diferentes Departamentos. Se desarrolla así un modelo centrado en el usuario independientemente de la complejidad administrativa.

El desarrollo de la Administración electrónica requiere de la colaboración entre las distintas Administraciones Públicas —Administración General del Estado, Administración Autonómica y Administración Local—, dado el modelo descentralizado de nuestro país. Muchos servicios básicos de e-europe 2005 que recomendaba la Comisión Soto exigían total o parcialmente la cooperación entre administraciones territoriales distintas. Esto obligaba a desarrollar una atención preferente a los municipios pequeños y medianos.

El proyecto administracion.es contenía un plan de choque, estructurado en cuatro grandes ejes de actuación.

El primero de ellos iba orientado a democratizar —a ampliar— el acceso a Internet y al certificado electrónico. Esto se ha mejorado especialmente a través del DNI electrónico. Se pasa de que el ciudadano tenga que pedir el certificado electrónico a que se lo den. También se ha facilitado el acceso público de los usuarios a Internet, a través de los municipios y en las oficinas de atención al ciudadano [(27)].

El segundo trataba de impulsar el desarrollo de servicios para los usuarios, en línea con el impulso de los servicios públicos electrónicos establecidos por la normativa UNE de eEurope 2005 [(28)]: cartas de servicio electrónicas, perfec-

27. En el año 2005 había 12.800.000 personas usuarias de Internet en España —el 34,6% de la población mayor de 14 años— y sólo había 700.000 con certificados electrónicos.

28. El Ayuntamiento de Madrid dio hace años la posibilidad de pagar impuestos o domiciliarlos por Internet mediante certificado electrónico —Impuesto sobre Vehículos de Tracción Mecánica, Impuesto de Bienes Inmuebles, Impuesto de Actividades Económicas—, de hacer altas y modificaciones al padrón municipal y de mecanizar la contratación administrativa a través de firma electrónica. La Comunidad de Madrid ha automatizado progresivamente la declaración de tributos, el registro de entrada, la solicitud de residencias y de prestaciones sociales —aunque no existe interconexión y se exija documentación complementaria—. También se puede matricular a los alumnos por Internet y el centro solicita tus datos a la Agencia Tributaria —aunque se exige documentación complementaria y no hay interconexión—.

cionamiento del Portal del ciudadano, pago de impuestos por Internet, formularios administrativos que se envían telepáticamente, etc. El desarrollo de la sociedad de la información exige un conjunto de servicios comunes necesarios para la tele-tramitación de procedimientos administrativos: servicios de autenticación de usuarios, registros telemáticos, sistemas de pago *on-line*, notificaciones telemáticas seguras, sistemas de archivo digital de documentación, accesibilidad de las páginas web, etc. (29).

El tercer eje iba orientado a facilitar el intercambio de información entre Administraciones Públicas. Así se pretendía la sustitución de certificados en papel que se obtienen de una Administración Pública y se presentan ante otra por certificados telemáticos y transmisiones de datos entre Administraciones Públicas. Se buscaba el establecimiento de un portal de servicios de la Administración General del Estado para las Entidades Locales, así como la creación de servicios denominados multi-agencia cuya prestación requiere la colaboración entre diferentes departamentos y organismos. Un portal único, como frontal de servicios para el ciudadano, exige unas interfaces comunes de las distintas Administraciones Públicas. Red.es tenía pensado establecer una plataforma de intercambio de datos, a partir de los desarrollos que se encontraban disponibles, como la pasarela de pago de la Agencia Española de Administración Tributaria o los módulos de pista —Ventanilla Única— (30). Esto exige procesos integrados entre las distintas Administraciones Públicas con interfaces comunes y servicios que coordinen el *back office*, así como la homogeneización de las diferentes aplicaciones informáticas (31). Sin embargo, la integración de las nuevas tecnologías en la comunicación interna de la Administración es lo más complejo porque obliga a ponerse de acuerdo en los distintos modelos de transacciones (32).

---

29. La Sociedad Estatal Correos y Telégrafos ha desarrollado una solución para prestar un servicio de Notificaciones Telemáticas Seguras del portal administracion.es <http://notificaciones.administracion.es/portalciudadano/acceso_servicio.asp>.

La Fábrica Nacional de la Moneda y Timbre presta diferentes servicios de certificación electrónica.

30. La Agencia Tributaria suministra habitualmente información por Internet a otras Administraciones Públicas. El Consejo General del Poder Judicial y el Ministerio de Justicia tienen proyectos interesantes de conexión de diferentes registros con los juzgados.

31. La necesidad de homologar las aplicaciones de los órganos jurisdiccionales es una exigencia que siempre han planteado las Instrucciones del CGPJ.

32. En el ámbito de la colaboración entre las Agencias de Protección de Datos hay que señalar que la Agencia de Protección de Datos de la Comunidad de Madrid ya formuló durante el año 2003 una propuesta que bus-

El cuarto eje va orientado a apoyar la reorganización interna de los procesos en las Administraciones Públicas: impulso al portal del empleado público, coordinación de las distintas Administraciones Territoriales, revisión de los procedimientos administrativos para su prestación telemática; establecimiento de sistemas de archivo de documentación electrónica. Así, ha habido distintos Planes Estratégicos de Simplificación de la Gestión Administrativa tanto en la Administración General del Estado como en las Comunidades Autónomas, que estaban implícitos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común [33].

El Ministerio de Administraciones Públicas lanzó en el año 2004 el Plan de Modernización Tecnológica de la Administración Pública 2004-2007 —*Plan Conecta*—, que sustituía al administración.es —dentro del más amplio España.es—. Este Plan recogió el último compromiso de la Administración General del Estado con las tecnologías y con los ciudadanos. Como señaló el Ministro de Administraciones Públicas, *«conectar es el motor de este Plan. Conectar Administraciones y conectar personas»* [34]. Este Plan se desarrolla en cinco grandes ejes —de los que forman parte 43 proyectos concretos—: Certifica, e-DNI, Ciudadano.es, Simplifica y Map.es.

Certifica pretende suprimir el 80% de los certificados que la Administración General del Estado exige a los ciudadanos, pero que están disponibles en otras Administraciones Públicas. De esta forma, se quiere reducir la burocracia, los trámites y las esperas injustificadas. La Agencia Tributaria, la Seguridad Social o el Registro Civil emiten millones de certificados en papel que se pretenden sustituir mediante certificados en Internet y un intercambio seguro

---

caba una mayor colaboración entre el Registro General de Protección de Datos de la Agencia Española y los Registros de Datos Personales de las Comunidades Autónomas. La Agencia elaboró diferentes documentos como la Propuesta de Modelo de transacciones, las especificaciones iniciales y las características generales del sistema y los formatos xml de intercambio de datos. Cfr. nuestro trabajo «La Administración independiente en la Comunidad de Madrid», en E. ÁLVAREZ CONDE y R. PLAZA DE DIEGO: *Derecho Público y Administración de la Comunidad de Madrid,* Tirant lo Blanch, Valencia, 2008, p. 1066, y la *Memoria de la Agencia de Protección de Datos de la Comunidad de Madrid 2004* —pp. 511-535— y *2003* —pp. 14, 158 y 525-527—.

33. Cfr. también *Administración electrónica. Gestiona tú mismo. Plan Estratégico de Simplificación de la Gestión Administrativa*, Comunidad de Madrid, 2001.

34. Este plan fue presentado por el Ministro de Administraciones Públicas Jordi Sevilla en el Tecnimap de 2004. Más información en <www.socinfo.info/contenidos/pdf8/conecta/pdf>.

de datos entre Administraciones. Desaparecerá progresivamente la necesidad de aportar documentos de forma reiterada a diferentes órganos de la Administración, lo que eliminará las colas y reducirá los tiempos de tramitación. Este es un proyecto prioritario porque cuatro o cinco certificados constituyen el 80% del total que la gente va a recoger a las ventanillas. Se pretende implantar la comunicación de cambios de domicilio y el servicio de e-notificaciones seguras —NTS—.

El *Documento Nacional de Identidad Electrónico* —e-DNI— permite a los ciudadanos identificarse y firmar en el mundo telemático y será la puerta de acceso segura a la identidad ciudadana única en la red. Con el e-DNI se pretende sustituir el DNI actual. El e-DNI incorpora la firma electrónica y ha estado operativo a partir de abril de 2006. Los proyectos representativos en este sector son la plataforma común de validación de firma electrónica y la identificación única.

Ciudadano.es es la marca bajo la cual el Gobierno quiere organizar nuevos espacios de reclamación, atención y comunicación con los ciudadanos: portales en la red, teléfonos de información u oficinas presenciales, múltiples canales conectados para un solo fin. Se pretende hacer del Ministerio de Administraciones Públicas un espacio de encuentro entre funcionarios y ciudadanos. Se crea así un portal general de atención al ciudadano, que incluirá la intercomunicación con las Administraciones con posibilidades de reclamación, atención y comunicación con los ciudadanos. Entre sus proyectos está la información pública electrónica, los centros de gestión unificada, la gestión integrada de ayudas y subvenciones, la pasarela de pago entre diferentes organismos públicos, el teléfono unificado de atención y el desarrollo de estaciones en el portal del funcionario.

Simplifica busca una gestión pública racional y eficiente, así como la reducción de tiempos de respuesta. Sus proyectos más representativos son el impulso de la imagen institucional, las licitaciones electrónicas y el observatorio de la administración electrónica. Se quiere cambiar los procedimientos, las formas de trabajar y definir los proyectos, facilitando la participación de los ciudadanos en su elaboración y evaluación, creando procedimientos orientados a los usuarios.

Map.es trata de actualizar y mejorar la tecnología de la Administración General del Estado, así como la unificación y potenciación de las páginas web de

la Administración del Estado. Entre sus proyectos se encuentra la red corporativa multiservicio del MAP, correo electrónico y directorio, formación virtual y firma electrónica para la gestión interna del MAP.

Con posterioridad el Ministerio de Administraciones Públicas puso en marcha el Plan de Medidas 2006-2008 para la Mejora de la Administración, denominado *Moderniza*. Este Plan consiste en 16 medidas que persiguen mejorar y modernizar la Administración para ponerla a la altura de las necesidades de los ciudadanos. En ellas se incluye iniciativas legislativas como la Ley de Administración Electrónica o el Estatuto básico del empleado, planes de acción como el Plan especial de medidas para la Administración General del Estado y la reforma de la Administración Periférica, el Plan de modernización tecnológica y simplificación administrativa de la Administración General del Estado y el Plan de medidas de promoción de la transparencia y la participación en la Administración General del Estado. Otras medidas eran la creación de un Observatorio de Calidad de los Servicios, la Red de Oficinas integradas —red 060— con CC.AA. y Ayuntamientos con más de 2.800 puntos de información; la unificación de los más de 1.000 teléfonos de atención ciudadana de la Administración General del Estado, la eliminación de más de 20 millones de documentos en papel entre 2006-2008; la incorporación a Internet de más de 800 nuevos formularios administrativos, conjuntamente con más de 100 nuevos servicios digitales accesibles con el nuevo DNI electrónico; el rediseño y simplificación de más de 300 trámites ciudadanos; la creación de foros de debate y participación de la actividad de la Administración General del Estado.

Durante el año 2006 el Gobierno ha tratado de desarrollar un conjunto de medidas enfocadas a facilitar la Administración electrónica: distribución del DNI electrónico, supresión de fotocopias de DNI y de los volantes de empadronamiento; o promoción de la colaboración entre administraciones mediante la creación de oficinas unificadas de atención a los ciudadanos [(35)]. 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 na-

35. Uno de los proyectos pioneros en este ámbito fue la inauguración en la Comunidad de Madrid durante el año 1999 de las ventanillas únicas empresariales en Getafe y Madrid —en la que tuve la oportunidad de participar—, espacios creados para favorecer la creación de empresas, configurando lugares donde estaban presentes la Administración General del Estado —Tesorería de la Seguridad Social y Agencia Tributaria—, la Administración de la Comunidad Autónoma, el Ayuntamiento y la Cámara de Comercio.

cional 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 (36). Para su puesta en marcha, es necesario que la Administración Pública ponga en funcionamiento dos Sistemas de Verificación de Datos, uno relativo a Datos de Identidad y otro relativo a Datos de Residencia, como establece la disposición final primera de los dos Reales Decretos, que no fija un plazo concreto para su realización. Hay que destacar también la aprobación de la modificación de la Ley Orgánica de Iniciativa Legislativa, que permitirá la recogida de firmas por Internet.

La Conferencia Ministerial Europea de noviembre de 2005 incorporó a su Declaración final la propuesta del Gobierno español de establecer criterios objetivos para evaluar el grado de avance de los trámites por Internet y de la Administración electrónica en cada país, un mecanismo similar al de los criterios de Maastricht que contribuyeron al éxito de la Unión Monetaria. Los países de la Unión Europea se comprometieron a realizar un seguimiento de su cumplimiento y a hacer públicos los resultados antes de la cumbre de Lisboa del año 2007. Se incluyó también el compromiso de los Estados miembros de fijar para el 2010 la posibilidad de que todos los ciudadanos comunitarios puedan acceder a los servicios telemáticos públicos de cualquier Estado de la UE con todas las garantías de seguridad. Esta Declaración Europea establece que en todos los estados miembros debe ser posible antes de 2010 la realización a través de Internet al menos del 50% de los trámites administrativos. Igualmente se recoge que la Administración Electrónica debe potenciar su papel como instrumento de integración social en la medida en que elimine la discriminación de acceso a los distintos servicios públicos (37). Uno de los ámbitos

---

36. Por tanto, no le es de aplicación a las Comunidades Autónomas y a los Ayuntamientos hasta que no aprueben un régimen jurídico similar.

37. La Agencia de Protección de Datos de la Comunidad de Madrid —como Administración Pública que es— ha puesto en marcha en el año 2005 el *Servicio para la declaración de ficheros por Internet mediante firma electrónica*. Este Servicio facilita la preceptiva declaración de ficheros de datos de carácter personal a todos los responsables de los ficheros de titularidad pública de la Comunidad de Madrid y es un buen ejemplo de la introducción de las nuevas tecnologías en la Administración. A través de este nuevo Servicio de Administración Electrónica, los responsables de ficheros pueden no sólo tramitar la inscripción de nuevos tratamientos en el Registro de Ficheros de Datos Personales de la Agencia, sino también acceder a los datos registrales completos de sus respectivos ficheros para su consulta, modificación, e incluso para la supresión de inscripciones. La Agencia de Protección de Datos de la Comunidad de Madrid se ha convertido así en la primera autoridad de

donde más iniciativas ha habido para el impulso de las nuevas tecnologías es el sanitario [38].

Recientemente se ha aprobado la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos —LAECSP—, que reconoce el derecho de todos *«a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 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»* —artículo 6.1 de la LAECSP—. Se trata no sólo de que las administraciones puedan ofrecer servicios, sino de que los ciudadanos tengan el derecho de exigirlos y puedan hacer sus trámites a través de la red [39]. Como 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*

---

protección de datos de España que permite la declaración de ficheros de datos personales a través de Internet con plena validez jurídica, mediante la utilización de certificados digitales personales y la firma electrónica de las declaraciones. Igualmente la Agencia está desarrollando proyectos orientados tanto a la mejora de los sistemas de información de la Agencia como a facilitar al responsable el cumplimiento de sus obligaciones y a mejorar las garantías de los ciudadanos. Entre los proyectos que buscan mejorar los sistemas de información, hay que destacar la mecanización del procedimiento de declaración de ficheros para su inclusión dentro del Plan de Simplificación de la Gestión Administrativa de la Comunidad de Madrid, lo que permitirá sobre todo la mejora en el seguimiento y en la información de los procedimientos de creación, modificación, supresión e inscripción de ficheros que se encuentren en tramitación. Entre los proyectos orientados a ayudar a los responsables de ficheros en el cumplimiento de sus obligaciones hay que mencionar el diseño de una herramienta dirigida a éstos que les facilite no sólo la declaración de los ficheros sino también el cumplimiento de otras exigencias legales —como, por ejemplo, la auditoría de seguridad o la posibilidad de facilitar el ejercicio de los derechos de acceso, rectificación y cancelación—. Entre los proyectos orientados a mejorar las garantías de los ciudadanos se encuentra la posibilidad de ejercer los derechos de acceso, rectificación y cancelación ante el responsable del fichero, la tutela de estos derechos y la denuncia ante la Agencia a través de Internet mediante firma electrónica.

38. Cfr. nuestra Introducción a *Protección de Datos Personales para Servicios Sanitarios Públicos,* Civitas-APDCM, Madrid, 2008, pp. 11-14.

39. Como hemos señalado anteriormente, el 45.2 de la LRJAP y 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»*. Este precepto *«deja[n] en manos de las propias Administraciones determinar si los ciudadanos van a poder de modo efectivo o no relacionarse por medios electrónicos con ellas, según que 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»* —apartado I—.

éstas de dotarse de los medios y sistemas electrónicos para que ese derecho pueda ejercerse. Esa 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» (40). 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 (41). 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 —artículos 24 a 26— que deroga la regulación existente de los registros telemáticos del artículo 38.9 LRJAP y PAC, subsistiendo la regulación de los registros generales en soporte informático establecida en el artículo 38.3 de la LRJAP y PAC. Esta Ley también lleva a cabo una precisa regulación de las notificaciones por medios electrónicos —artículo 28— que deroga la regulación de las antes denominadas notificaciones telemáticas establecida en el

40. 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.

41. 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»*.

artículo 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 (42).

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»* —artículo 6.2.b) de la LAECSP—. Hay que recordar que el artículo 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 (43), lo que obliga a la utilización de las tecnologías de la información

---

42. 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 artículo 59.4 de la LRJAP y 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.

43. 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»* —apartado 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 […]»* —artículo 9.1—.

en las relaciones entre las Administraciones Públicas con un nivel adecuado de interoperabilidad de los sistemas de información [44]. 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»* —artículo 6.2.a) de la LAECSP— [45]. La LAECSP reconoce también el ejercicio por medios electrónicos de otros derechos que ya se encontraban en el artículo 35 de la LRJAP y PAC [46]. 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»* —artículo 6.2.b), desarrollado después en el artículo 37— y a *«obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado»* —artículo 6.2.e)—, que se encontraban previstos en el artículo 35.a) y c) de la LRJAP y PAC. También se reconocen otros derechos como el de *«la conservación en formato electrónico por las Administraciones Públicas de los documentos elec-*

---

44. 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»* —artículo 4.e)—. El Anexo de la LAECSP —apartado 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»* —artículo 40.2.a)—. Así, se establece 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. 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 —artículos 41-43— sobre la cooperación en materia de interoperabilidad de sistemas y aplicaciones. La interoperabilidad de los distintos registros de ficheros es una cuestión que hemos mencionado anteriormente.

45. La LAECSP contiene un Anexo de definiciones entre las que se encuentra la de canales —apartado 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 vía SMS y la propia Televisión Digital Terreste —apartado III—.

46. La LAECSP no modifica la regulación de las disposiciones generales sobre el procedimiento administrativo contempladas en el Título IV de la LRJPAC. Sin embargo, como señala Sánchez Navarro, el recurso de la Administración a las nuevas tecnologías, así como la mayor simplificación administrativa, también deben suponer una reducción de los plazos para algunos procedimientos establecidos en la LRJAP y PAC. Cfr. A. SÁNCHEZ NAVARRO, loc. cit., p. 107.

trónicos que formen parte de un expediente» —artículo 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»* —artículo 6.2.g)—, el de *«la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas»* —artículo 6.2.h)—, el de *«la calidad de los servicios públicos prestados por medios electrónicos»* —artículo 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»* —artículo 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 [47]. Es competencia exclusiva del Estado regular las bases del régimen jurídico de las Administraciones públicas que garantiza a los administrados un tratamiento común ante ellas y el procedimiento administrativo común, sin perjuicio de las especialidades derivadas de la organización propia de las Comunidades Autónomas —artículo 149.1.18.ª de la CE—. 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 ellas *«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»* —artículo 1 de la 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 todas las administraciones forme parte de ese tratamiento común que tienen»* —apartado II—.

47. La disposición final primera establece los preceptos de la Ley que tienen un carácter básico.

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»* —artículo 3.6 de la LAECSP—. Además, uno de los principios de la Ley es el 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»* —artículo 4.j)— [48]. 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»* —artículo 34—.

3. LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA

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 África [49]. 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.

---

48. 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 —artículo 33.1— y como uno de los elementos que deben garantizar las aplicaciones y sistemas de información utilizados para la instrucción por medios electrónicos —artículo 36.1—.

49. Cfr. también A. TRONCOSO REIGADA, Introducción, *Manual de Protección de Datos para las Administraciones Públicas*, Civitas, Madrid, 2004.

El recurso a las nuevas tecnologías no debe perjudicar la relación 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 (50). Hay que señalar que el artículo 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 (51). 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 (52), así como a través de medidas técnicas que favorezcan la accesibilidad para las personas que tengan algún tipo de

---

50. Como señala la Exposición de Motivos, *«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.

51. 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»* —artículo 4.b)—.

52. La Exposición de Motivos de la LAECSP insiste en que el derecho de los ciudadanos a relacionarse con la Administración a través de medios electrónicos implica *«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 remita la Administración Pública»* —apartado II—. En esta dirección, el artículo 8 de la LAECSP, «Garantía de prestación de servicios y disposición de medios e instrumentos electrónicos», obliga a las Administraciones 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 hacen mención el apartado III de la Exposición de Motivos y la disposición adicional segunda.

discapacidad [53]. 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 [54]. La LAECSP afirma también una suerte de principio de igualdad para las 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»* —artículo 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. Este principio también se encuentra también en el artículo 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 *«por que 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»* —artículo 14.1—.

3.1. EL INCREMENTO DE LOS TRATAMIENTOS DE DATOS PERSONALES EN LA ADMINISTRACIÓN ELECTRÓNICA. LAS TECNOLOGÍAS DE PROTECCIÓN DEL DERECHO A LA INTIMIDAD

El riesgo más importante es que la Administración electrónica suponga una vulneración de la privacidad personal y, en especial, del derecho fundamental

53. La LAECSP proclama así un principio de accesibilidad a la información —artículo 4.c)—.

54. En todo caso, el modelo tradicional de participación social dista de ser transparente y se presta a la actividad de grupos de presión.

a la protección de datos personales [55]. Las personas son cada vez más conscientes y cautelosas con sus datos personales y tienen una mayor sensibilidad sobre su protección, 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 —artículo 18.4 de la CE—. Como hemos señalado anteriormente, 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. Lógicamente, la utilización de medios y técnicas electrónicas, informáticas y telemáticas en las Administraciones Públicas lleva aparejado el almacenamiento y tratamiento automatizado de la información personal, pues en caso contrario perdería sentido la utilización de este tipo de medios y técnicas. Y 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. Pues bien, los principios y derechos de protección de datos son plenamente aplicables a la Administración electrónica [56]. De hecho, se puede afirmar que no sólo es posible hacer compatibles la eficacia e inmediatez de los servicios de

---

55. 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*, núm. 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*, núm. 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*, núm. 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* núm. 3, 2007, pp. 95-169. Quisiera destacar el borrador de Recomendación de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica, que traspone algunas ideas que hemos tenido la posibilidad de exponer en *La protección de de datos personales. En busca del equilibrio*, Tirant lo Blanch, Valencia, 2006.

56. 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 Pro-

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 sociedad y en las Administraciones Públicas (57).

---

yecto 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 tiene como objetivos la ciberseguridad y el establecimiento de servicios públicos interactivos para todos— trató de promover la necesidad de garantizar el derecho fundamental a la 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 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 interacciones bidireccionales 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 concretas circunstancias 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 adecuado nivel 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 la existencia de 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.

57. Sobre la cuestión existe un interesante Documento de trabajo del Grupo de Protección de datos del artículo 29, relativo a la administración en línea, adoptado el 8 de mayo de 2003 —<http://www.europa.eu.int/comm/ privacy>— ya citado. 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. Es-

La Ley 24/2001, de 27 de diciembre, de medidas fiscales, administrativas y de orden social, que modifica la LRJAP y PAC, lleva a cabo ya una referencia a la legislación de protección de datos personales en el ámbito de la Administración electrónica. Así, esta Ley incorpora un Disposición adicional decimoctava relativa a la Presentación telemática de solicitudes dirigidas a la Administración General del Estado y sus Organismos Autónomos, donde se señala —apartado 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»*. Además, 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»* —artículo 34— [58]. En todo caso, no bastaba una simple remisión a la legislación de protección de datos personales, cuyos principios y derechos no pueden ser afectados; era también necesaria una legislación específica que abordando la administración electrónica, establezca a través de medidas concretas, la vigencia de los principios y derechos de protección de datos personales en este ámbito.

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

---

te documento aborda cuestiones como el establecimiento de puntos de entrada únicos a los serviciosde 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>.

58. 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 artículo 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 desarrollo»*. Hay múltiples menciones a la legislación de protección de datos en este Reglamento.

transparencia de estas tecnologías —apartado 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»* —artículo 3.3—. En esta dirección, la Exposición de Motivos de la LAECSP señala que 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 —apartado III—. Igualmente señala 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 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»* —apartado V—. 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 Administración 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»* —artículo 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 —artículo 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»* —artículo 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 —artículos 62.1 y 63 de la LRJAP— [59].

En todo caso, 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 esté fabricado de una manera que permita el control de los propios datos personales [60]. Esta es una cuestión a la que se ha referido la Directiva 2002/58/CE, de 12 de julio de 2002 —artículo 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»* [61]. 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»* [62]. Si bien la tecnología no basta por sí sola para

---

59. Cfr. M. FERNÁNDEZ SALMERÓN: *La protección de los datos personales en las Administraciones Públicas*, cit., pp. 465 a 470.

60. 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.

61. 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».*

62. 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 de mayo de 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

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 (63). Hay

---

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 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 a la Comunicación de la Comisión sobre el papel de la administración electrónica en el futuro de Europa —COM (2003) 567 final, de 26 de septiembre de 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 he hecho mención con anterioridad.

63. 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*, núm. 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.

que mencionar especialmente la creación de sellos europeos de privacidad de productos y servicios(64).

Hay que señalar que la utilización de las nuevas tecnologías supone un incremento de los tratamientos de datos personales realizados por las Administraciones Públicas. La posibilidad de iniciar procedimientos administrativos a través de Internet, aunque después se proceda al almacenamiento manual de la información, obliga a que los correspondientes registros electrónicos —para la recepción o salida de las solicitudes, escritos y comunicaciones— sean creados, como ficheros informáticos que son, a través de una disposición de carácter general —artículo 20 de la LOPD— (65). En esta dirección hay que

64. 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. El proyecto Europrise sigue inicialmente el modelo establecido por la Autoridad de Protección de Datos de Schleswig-Holstein, establecido en el año 2000 y que ha permitido hasta la fecha certificar más de 45 productos. 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».*

65. El tratamiento de datos consistirá únicamente en facilitar la rcepción de las solicitudes planteadas por los ciudadanos, sin acceder a su contenido, dando traslado al órgano competente para el inicio y tramitación del procedimiento. En muchas ocasiones, este fichero de registro ya está declarado, siendo necesaria una modificación de la declaración para adecuar el sistema de información. Algo semejante ocurre en el caso del DNI-e. Este es un fichero informatizado de datos personales que debe estar declarado a través de una disposición de carácter general. 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.

señalar que 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 —artículo 25.1—(66). Este órgano tendrá, a nuestro juicio, el carácter de responsable del fichero del registro electrónico a los efectos de la LOPD, con independencia de cuál sea el órgano administrativo competente para la efectiva tramitación del procedimiento que se inicie, sea la tramitación electrónica o no. 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 (67). El expediente electrónico, al que hace referencia el artículo 32 LAECSP, debe ser considerado también un fichero de datos de carácter personal. La Administración pública puede optar por una tramitación parcial por medios electrónicos, imprimiéndose algunos documentos en soporte papel, e incluso optar por un tratamiento mixto o parcialmente automatizado (68). Igualmente, la recogida de *cookies* supone un tratamiento de datos personales (69), que, sin perjuicio del derecho a la información y el consentimiento del interesado al que después nos referiremos, debe ser declarado a través de una disposición de carácter general. Si bien la dirección IP no siempre es estática sino que puede ser dinámica, además de

66. Ha desaparecido la previsión del artículo 45.4 de la LRJAP y 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»*.

67. El tratamiento consiste en el inicio, seguimiento y tramitación de las solicitudes de los ciudadanos. El responsable del fichero es el órgano que tenga la competencia para su resolución. No olvidemos que el artículo 44.3.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 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.

68. También supone un tratamiento de datos personales la creación, gestión y mantenimiento de repositorios de información o documentales, para el uso por diferentes órganos de la misma o de distinta Administración Pública. Este tratamiento de los datos consiste en gestionar el repositorio de datos o documental generado como servicio horizontal que permite a los ciudadanos el ejercicio de los derechos previstos en la LAECSP. El responsable del fichero puede ser el órgano administrativo al que se le encomiende la gestión del repositorio, tal 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.

69. Las *cookies*, con independencia de la información almacenada en ellas, puede vincularse con el usuario de un determinado dispositivo conectado a Internet y permite obtener su perfil. Normalmente, el responsable del fi-

que no identifica a un usuario sino un equipo —que puede ser de utilización compartida [70]—, en muchas ocasiones es una *«información concerniente a personas físicas identificadas o identificables»* —artículo 3.a) de la LOPD— [71].

---

chero 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.

70. 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.

71. 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. 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, ya citado, pp. 9-1.1Como 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 identificados 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»*. 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 periodo determinado, alegando el 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 estableci-

También suponen tratamientos de datos personales otros servicios de Administración electrónica fuera del ámbito de los procedimientos administrativos. Nos referimos a los servicios 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— y que deben ser declarados a través de una disposición de carácter general [72].

Hemos ido señalando quién es el responsable de cada uno de los tratamientos, que es, como señala el art. 5.1.q) del Reglamento de desarrollo de la LOPD, el órgano administrativo que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realice materialmente. Este órgano administrativo tiene la consideración de responsable, aunque no lleve a cabo materialmente el tratamiento sino que se apoye en un encargado, una cuestión que analizaremos posteriormente.

3.2. EL PRINCIPIO DE CALIDAD. LA FINALIDAD DEL DNI ELECTRÓNICO Y LOS DATOS OBJETO DE TRATAMIENTO

La Administración electrónica tiene que tener en cuenta especialmente el principio de calidad —artículo 4 de la LOPD—. Es muy importante que los datos sólo se utilicen para la finalidad para la cual han sido recabados y no para finalidades incompatibles —artículo 4.2 de la LOPD— y que sólo se traten aquellos datos que sean adecuados y pertinentes para esa finalidad, no debiéndose

---

do 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"»*.

72. Esto mismo ocurre cuando se recogen datos personales en procesos de participación social por medios electrónicos —donde se solicita a los ciudadanos su opinión sobre distintas actuaciones administrativas— o en *blogs* y foros de discusión 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.

almacenar en ningún caso datos excesivos —artículo 4.1 de la LOPD— [73]. Si las tecnologías de la información permiten 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 [74]. Aunque los principios de protección de datos, y, en concreto, el principio de calidad, también afecta a los tratamientos de datos personales no automatizados, el hecho de que los datos personales derivados de la propia tramitación administrativa van 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»* —apartado III—. Así, como señalaremos más adelante, la LAECSP señala en relación con la transmisión de datos entre Administraciones Públicas que la disponibilidad de tales datos *«estará* limitada

---

73. El documento de trabajo del Grupo del Artículo 29 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, no se deberían pedir ni almacenar datos personales excesivos o fuera de propósito, que probablemente no tendrán aplicaciones legítimas y pertinentes en el servicio público.

De esta forma, los datos aportados por el ciudadano al iniciar un procedimiento por medio de un servicio de administración electrónica, o los que se obtengan por medio de elaboraciones de los mismos o a través de actos de trámite del correspondiente procedimiento deben estar vinculados a éste, no pudiendo ser utilizados por otros servicios o dependencias de la Administración en cualquier otro expediente. Igualmente, es excesivo el tratamiento de los datos recibidos en las sedes electrónicas o registros telemáticos con cualquier finalidad distinta de la simple puesta a disposición del órgano en que resida la competencia para la tramitación del expediente administrativo o servicio solicitado por el interesado. Cfr. el borrador de Recomendación de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica.

74. Así, por ejemplo, es importante que en los instrumentos de participación social, así como en los *blogs* y foros de discusión, se recojan únicamente los datos personales estrictamente necesarios —por ejemplo, el correo electrónico— para poder participar y opinar en dichos foros. 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 expresadas por los ciudadanos se encuentran protegidas por el artículo 20.1 de la CE que reconoce y protege el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra o el escrito o cualquier otro medio de reproducción, sería contrario al principio de calidad verter opiniones que menoscaben el derecho al honor y a la intimidad de otras personas. Estos datos pueden ser suprimidos por el Administrador del foro.

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»* —artículo 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. La LAECSP establece expresamente 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»* —artículo 4.g)—.

Hemos señalado anteriormente que cada Administración Pública es una personalidad jurídica única, por lo que los accesos de los distintos departamentos están sometidos al principio de calidad, no tratándose de una cesión de datos personales. A diferencia del artículo 35.f) de la LRJAP y PAC, 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»* —artículo 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.

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»* —artículo 4.3 de la LOPD [75]—. Esto es especialmente importante en un ámbito como el de la Administración electrónica donde

75. Es muy importante la exactitud de la información que se maneja en la Administración electrónica. Así cuando de los datos recogidos en la solicitud de un servicio de administración electrónica o, de la verificación o comprobación de los mismos, se detecte la inexactitud de cualquier información almacenada en el fichero que soporte el servicio, se debe proceder a la corrección de los mismos. Si los datos objeto de corrección se hubieran facilitado a cualquier otro órgano administrativo, se debe poner en su conocimiento la rectificación realizada, al objeto de que se proceda a las correcciones necesarias. Cfr. el borrador de Recomendación de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica.

los datos —por ejemplo, de los registros y 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»* —artículo 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»* —artículo 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»* —artículo 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»* —artículo 28.2—. Igualmente, para que las copias de documentos realizadas por medios electrónicos tengan la consideración de copia auténtica con la eficacia prevista en el artículo 46 de la LRJAP y PAC, con independencia de cual 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 —artículo 30.1—. Es especialmente importante, como después señalaremos, la seguridad de la información en el ámbito de la Administración electrónica, que garantice su integridad y autenticidad.

El principio de calidad obliga a almacenar los datos *«de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados»* —artículo 6 de la LOPD [76]—. Sin duda, la Administración electrónica facilita el almacenamiento de la información personal, permitiendo el acceso a los propios datos personales. Por otra parte, la LAECSP reconoce a los ciudada-

76. 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, deben conservarse la fuente de los distintos datos —facilitados por el propio interesado, generados por los actos de trámite o resolutorios del procedimiento, otras fuentes, etc.—. Así, es conveniente la conservación de la trazabilidad acerca del origen de los datos y su destino.

nos el derecho a la *«conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente»* —artículo 6.2.f)—. Igualmente, el artículo 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»* (77). 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»* —artículo 4.5—. No corresponde a la LAECSP establecer el plazo de conservación de los documentos electrónicos, sino que esto corresponde a la legislación administrativa correspondiente. Sin embargo, las posibilidades técnicas no justifican una conservación ilimitada de los documentos electrónicos cuando no tengan ya valor probatorio o hayan transcurrido los plazos señalados por la legislación sectorial (78). Los medios electrónicos sí son una ayuda importante para el mantenimiento íntegro de los datos *«atendiendo los valores históricos, estadísticos o científicos»* —artículo 4.5, último párrafo—.

El principio de calidad anima a no conservar los datos *«en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados»* —artículo 4.5, segundo párrafo de la LOPD—. No se trata sólo de 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 automática de los datos pasado el plazo necesario para el cumplimiento de la finalidad (79). Así, por ejemplo, las personas que utilicen comunicaciones

77. El almacenamiento de documentos electrónicos que contegan 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 —artículo 31.2 de la LAECSP—.

78. Es razonable la supresión de la información de un repositorio común pasado un plazo razonable. En todo caso, el hecho de que se termine un procedimiento no implica que se tengan que borrar los datos del repositorio, pues estos repositorios tienen como finalidad almacenar datos que sirvan para diferentes procedimientos administrativos. Si se suprime la información, se priva de su utilidad para otro procedimiento distinto que puede iniciar el ciudadano.

79. 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*

electrónicas puedan permanecer no identificados 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 (80). En este sentido, era importante la cancelación de los datos de tráfico o su anonimización, una vez cumplida la finalidad de la comunicación o su facturación (81). 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 (82). Sin embargo, el interés público en la protección de los datos 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. De esta manera, 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 la anterior Directiva 2002/58/CE, permite la conservación de los datos de tráfico por un plazo de tiempo más amplio para proteger la seguridad nacional, la de-

---

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».*

80. 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.

81. 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.

82. 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 —artículo 12—.

fensa, 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 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 —artículo 1—.

El DNI electrónico ha planteado un conjunto de implicaciones en relación con la protección de datos personales [83] y, en especial, respeto al principio de calidad —la finalidad del DNI electrónico y los datos personales que pueden ser tratados— [84]. La Ley Orgánica 1/1999, de 21 de febrero, de Protección de la Seguridad Ciudadana establece los principios básicos sobre tenencia y utilización del

83. 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»*.

84. 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. Núm. 254, año 2005—.

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 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 artículo 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 —artículo 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 artículo 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 [85]. 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 [86]. Todos los datos se tratan para acreditar la identidad y permitir la firma electrónica de documentos. Si bien existe una preocupación por el tratamiento de los datos biométricos, hay que señalar que

85. 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.

86. 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. Estos 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, entonces 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.

éstos cumplen la finalidad de identificación [87]. 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.

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 [88]. 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 [89]. 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

87. Cfr. nuestra Introducción a *An approach to data protection in Europe,* cit.

88. Véase la comparecencia del Director de la Agencia Española de Protección de Datos antes citada.

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

el saldo de puntos, que dispone una habilitación expresa en la Ley 17/2005, de 19 de julio, que regula el permiso y la licencia de conducción por puntos. 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 (90). En ningún caso parece razonable el uso del DNI-e con fines comerciales (91).

3.3. LA INFORMACIÓN Y EL CONSENTIMIENTO. SERVICIOS DE NOTICIAS Y ALERTAS Y USO DE COOKIES

La Administración electrónica debe tener en cuenta el principio de información —artículo 5 de la LOPD—. El ciudadano que utilice estos medios o soportes informáticos para relacionarse con la Administración Pública tiene que estar informado previamente de que sus datos personales van a ser incluidos en un fichero informático, de la finalidad del tratamiento de sus datos, de los destinatarios de la información, de la identidad y dirección del responsable del

---

90. 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*, núm. 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 puede ser utilizado 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*, núm. 128, 2005, pp. 683 a 694.

91. 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, muchos países prohíben en sus legislaciones la existencia de un número único de identificación de los ciudadanos.

fichero y de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. 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 el consentimiento del interesado. De esta forma, el principio de información permite mejorar la confianza del ciudadano en la Administración en línea (92).

Es especialmente importante la información al ciudadano sobre las cesiones de datos entre Administraciones Públicas —accesos electrónicos, interconexiones—, especialmente cuando estas cesiones se realizan sin su consentimiento ya que sólo conociendo quién tiene sus datos personales puede el ciudadano controlar de alguna manera el uso de su información personal (93). Por ello, es necesario informar al interesado cuando formule solicitudes por medios electrónicos en las que declare datos personales que obren en poder de las Administraciones Públicas de la posibilidad que tiene el órgano destinatario de la solicitud para efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la autenticidad de los datos, una previsión que se encuentra en el art. 11 del Reglamento de desarrollo de la LOPD y que después analizaremos. 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 —artículo 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

92. Así, por ejemplo, cuando se recaban datos como la firma electrónica, hay que informar a los ciudadanos en los términos previstos en el artículo 5.1 de la LOPD. Lo mismo debe hacerse en la recogida de datos personales para la gestión de altas en los servicios de novedades o de alertas SMS.

93. 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 *«facilitaran al usuario información clara acerca de la comunicación de los datos, en cumplimiento de las normas de comunicación de datos personales»*.

al número de interesados o a la antigüedad de los datos —artículo 5.5 de la LOPD— [94].

Hay que prestar una especial importancia a la política de privacidad en los sitios web de las Administraciones Públicas [95]. Así, por ejemplo, debe informarse al ciudadano de la posibilidad de comprobar en otros ficheros de la Administración Pública la veracidad de un documento presentado a la Administración Pública [96]. Igualmente, la utilización de *cookies* supone un tratamiento de datos personales que requiere siempre el cumplimiento de este principio de información del interesado sobre su existencia —que la mayoría de las veces desconoce—, de su finalidad, de los destinatarios de la información, de la identidad del responsable y de 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 —artículo 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*

---

94. Cfr. E. GUICHOT REINA: *Datos personales y Administración Pública*, cit., pp. 390 y 391.

95. Así, en la página de inicio de los sitios web debería aparecer *«Política de privacidad»,* ofreciendo una información fácilmente comprensible de la titularidad del sitio web, de su finalidad, 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. Especialmente, cuando se vaya a recoger datos personales, deberá contener una leyenda en los términos establecidos en el artículo 5 de la LOPD.

96. Así, por ejemplo, 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, reconocido en la Ley 11/2007, de 22 de junio, se deberá informar expresamente de tal hecho al ciudadano. Cfr. el Cfr. el borrador de Recomendación de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica.

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» (97).

No obstante, la introducción de las nuevas tecnologías es también una oportunidad para el mejor cumplimiento de este principio de información. Es necesario que en cada formulario electrónico se indique la existencia de un tratamiento de datos personales en el Registro, su finalidad, la comunicación de los datos a otros órganos, quién es el responsable y los derechos del interesado. Si bien los impresos o solicitudes donde se recaban los datos disponen en ocasiones de leyendas informativas, la tramitación telemática ofrece una oportunidad a los poderes públicos para informar, impidiendo, por ejemplo, el envío de la solicitud si no se ha leído la cláusula informativa(98). Esta información debe ofrecerse al interesado cuando visita la oficina virtual, de manera que no pueda presentar un escrito sin que la Administración haya cumplido el deber de información. Así, en la Comunicación que recientemente la Comisión ha enviado 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) —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, contribuye a garantizar que el interesado autoriza el tratamiento de sus datos con conocimiento de causa»* (99).

---

97. Igualmente, hay que cumplir el principio de información del art. 5.1 LOPD cuando se recaban datos personales —por ejemplo, la dirección de correo electrónico— para la participación en foros de discusión y blogs.

98. Así, por ejemplo, para facilitar la información se puede acceder a una ventana que contenga un texto informativo específico sobre los datos 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 información y bloqueando el acceso al servicio en el caso de que no se haya marcado y visualizado la ventana correspondiente. Cfr. el borrador de Recomendación de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica. Además, los medios electrónicos también pueden ser utilizados para cumplir la obligación del responsable del fichero de conservar la prueba que acredita el cumplimiento del deber de información —como ha establecido el Reglamento de desarrollo de la LOPD—.

99. COM (2007) 228 final, de 2 de mayo de 2007 —loc. cit.—.

La utilización de las nuevas tecnologías permite materializar el consentimiento del interesado para el tratamiento de sus datos —artículo 6.1 de la LOPD—. Esto es especialmente importante en los tratamientos llevados a cabo por responsables de ficheros privados ya que se puede facilitar la prueba de la dación del consentimiento. En el caso de la Administración electrónica y al tratarse de funciones administrativas no es preciso recabar el consentimiento del interesado para el tratamiento de sus datos personales —artículo 6.2 de la LOPD— [100]. Además, la existencia de una relación administrativa justifica también el tratamiento de los datos personales contenidos en la información facilitada por el interesado que son necesarios para su mantenimiento y cumplimiento, como ocurre en muchas ocasiones en el ámbito del portal del empleado.

No obstante, 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 medios electrónicos—, 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 la tramitación de un procedimiento administrativo 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»* —artículo 27.2—. Cuando la tramitación es iniciada de oficio por la propia Administración Pública, los interesados deben otorgar expresamente su consentimiento, o bien realizar actos de los que se desprenda esta aceptación. Además, aunque el procedimiento haya sido iniciado por medios electrónicos, el ciudadano —e incluso terceros interesados— puede optar por una tramitación no electrónica por lo que 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, que también podrán emitirse y recabarse por medios electrónicos —artículo 28.1 de la LAECSP—. Es

100. Así, por ejemplo, las sedes electrónicas y los registros telemáticos que permiten el acceso a servicios de administración electrónica, a instancia del interesado, no necesitan recabar el consentimiento del interesado para el tratamiento de sus datos.

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 tenga efectos jurídicos. 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 concertados en un registro previo —artículo 13 de la LAECSP—, lo que permite otorgar plena eficacia jurídica a los documentos firmados electrónicamente (101). Este es el caso también cuando se pretende el acceso a un expediente administrativo o cuando se procede a firmar durante el procedimiento electrónico los documentos contenidos en las pruebas documentales (102).

La Administración Pública también recoge datos personales para ofrecer determinados servicios administrativos y donde es necesario el consentimiento del interesado (103). Este es el caso de la recogida de datos personales de suscriptores de servicios de noticias —*newsletter*— o de alertas SMS o MMS (104). 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

---

101. 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 persona.

102. 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.

103. Este consentimiento puede ser recabado dando la posibilidad de marcar una casilla específica, por el interesado, que previamente no esté marcada, en el formulario en el que se acceda al servicio de Administración electrónica. Cfr. el borrador de Recomendación de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica. En todo caso, este consentimiento puede ser revocado en cualquier momento, como señala el Reglamento de desarrollo de la LOPD.

104. También es necesario el consentimiento del ciudadano para el tratamiento de sus datos y para su difusión en el ámbito de *blogs* y foros de discusión, aunque puede ser un consentimiento tácito, después de haber sido informado. Es recomendable utilizar algún sistema de identificación que permita verificar la identidad de las personas que dicen ser las autoras de las opiniones y de las informaciones. En relación con los menores de catorce años, debe articularse un procedimiento que garantice que cuando pretendan suscribirse a un foro se obtenga el consentimiento de la persona que ejerza la patria potestad o tutela.

las denominadas *cookies*— sobre los itinerarios que siguen los ciudadanos al visitar los sitios web de la Administración —que 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 (105). La finalidad de esta medida es tratar de mejorar la información que las Administraciones Públicas ofrecen en Internet e, incluso, ofrecer 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 la información 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 artículo 6.3 de la Directiva 2002/58/CE (106) y no supone el ejercicio de una función administrativa por lo que se requiere el consentimiento del interesado (107). Existe un derecho a la información administrativa —artículo 35.g) de

---

105. 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*, núm. 3, 2003, pp. 176-177. La utilización de *cookies* ha sido analizada por el Grupo de Trabajo del Artículo 29 en el documento «Privacidad e Internet: enfoque 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>.

106. *«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».*

107. 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 de mayo de 2007— que menciona como una de las formas de PET establece que *«los anuladores de cookies, que bloquean las cookies introducidas en un ordenador para que lleve a cabo deter-*

la 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— (108). 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 esa información sin necesidad de la 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 —artículo 4.b)—. Por tanto, sólo si existe consentimiento del interesado puede producirse la utilización de *cookies* en los sitios web de la Administración Pública. Lógicamente el consentimiento del interesado no tiene que ser expresado a través de un medio de identificación fuerte sino que basta con que éste sea libre, inequívoco, específico e informado, puede ser tácito (109).

---

minadas 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.

108. 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.

109. 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, deberá habérsele advertido expresamente de esta circunstancia, 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.

3.4. LOS ACCESOS ELECTRÓNICOS, LAS INTERCONEXIONES Y EL RESPETO AL PRINCIPIO DE PROPORCIONALIDAD

Mención específica merecen 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 [110], *«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 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 —sobre todo de comodidad— para el ciudadano 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 suprimen de hecho la intimidad y el libre desarrollo de la personalidad, 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 [111]. 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 de Protección de Datos establece que los datos de carácter per-

110. Cfr. la Introducción del Documento de trabajo sobre la administración en línea, de 29 de enero de 2003, ya citado.

111. 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 en los individuos, que deriva principalmente de las interconexiones.

sonal sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario con el previo consentimiento del interesado, salvo que la cesión esté autorizada por Ley —artículo 11 de la LOPD—[112]. La comunicación de datos sólo puede producirse entre Administraciones Públicas cuando exista consentimiento del interesado o una habilitación legal. La Administración electrónica no es una excepción, por lo que sólo es posible la comunicación de datos con el consentimiento del interesado —que también puede ser expresado por medios electrónicos— y la habilitación legal. A nuestro juicio, no se trata tanto de establecer una prohibición de las interconexiones sino de exigir que exista una habilitación legal —que debe producirse cuando exista un interés público— o el consentimiento del interesado. No hay que olvidar que la Administración electrónica debe respetar la regulación específica del consentimiento para los datos especialmente protegidos —artículo 7 de la LOPD—. Además, la previsión legal o la propuesta del consentimiento del interesado debe respetar en todo momento el principio de calidad —al que más adelante nos referiremos— y el principio de proporcionalidad [113], 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

---

112. Así, 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 administrativos de la Administración General del Estado y de 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 interesado para que los datos puedan ser consultados por este sistema por el órgano instructor, debiendo constar dicho consentimiento en la 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 prestanción 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 LRJAP y 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»*.

113. Cfr. M. MEDINA GUERRERO: «El principio de proporcionalidad», *Cuadernos de Derecho Público*, núm. 5, 1998 y M. GONZÁLEZ BEILFUSS: *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional*, Aranzadi, Pamplona, 2003. Esta cuestión la hemos analizado en A. TRONCOSO REIGADA: Introduction a *An Approach to Data Protection in Europe*, Thomson-Civitas/APDCM, Madrid, 2007, pp. 33-36.

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 (114). También, es necesario llevar a cabo un juicio de necesidad que tenga en cuenta si existen otros posibles medios que permitan alcanzar ese interés público y la ventaja de los ciudadanos con 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 —al que después nos referiremos—, se echa en falta una regulación más específica sobre la interconexiones de datos personales. Es necesario que las Autoridades de Protección de Datos informen preceptivamente la solicitudes de interconexión y que las Administraciones Públicas introduzcan todas las garantías posibles —por ejemplo, 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.

La legislación española relativa a la Administración electrónica siempre ha exigido que el acceso y la interconexión de datos entre Administraciones Públicas se haga sólo con el consentimiento del interesado —que también puede ser expresado por medios electrónicos— o a través de una habilitación legal (115). La LAECSP reconoce el derecho *«[a] no aportar los datos y docu-*

---

114. 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»*.

115. 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 LRJAP y PAC —derogada por la LAECSP— señalaba 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*

mentos 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. El citado consentimiento podrá emitirse y recabarse por medios electrónicos» —artículo 6.2.b)— [116]. Por tanto, en nuestro país, el intercambio de certificados y la transmisión de datos entre Administraciones Públicas distintas exige la habilitación legal o el 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

---

la cesión de los correspondientes datos al órgano gestor por parte de las Entidades competentes». Igualmente 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».* Igualmente, la Disposición Adicional Cuarta de la Ley 40/1998, de 9 de diciembre, Reguladora del Impuesto sobre la Renta de las Personas Físicas 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 de febrero, por el que se regulaban los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos, que introduce un artículo 14 en el 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 establece 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».*

116. La Exposición de Motivos de la LAECSP establece que este consentimiento tiene que ser expreso —apartado VI—, lo que no es una exigencia de la LOPD.

estaremos hablando realmente de comunicación entre Administraciones Públicas— [117].

Hay que recordar que la LOPD también 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»* —artículo 11.2.c) de la LOPD—. Esta previsión habilita las comprobaciones automatizadas por parte de las Administraciones Públicas de la información aportada por los ciudadanos, lo que implica la legitimación para la comunicación de datos entre Administraciones Públicas aunque ejerzan competencias diferentes. Este mismo criterio se encuentra recogido en el artículo 11 del Reglamento de desarrollo de la LOPD —«Verificación de datos en solicitudes formuladas a las Administraciones Públicas»— que señala 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».* De hecho, 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».* Igualmente 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»* —artículo 35—.

---

117. Cfr. sobre la cuestión —con un planteamiento distinto al nuestro— M.ª 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,* núm. 12, 2004, para quien *«la generalización del consentimiento de la persona concernida parece una garantía totalmente 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.

Por tanto, esta comunicación de datos personales para proceder a la verificación de la informacion dispondría también de la excepción de la habilitación legal prevista en el artículo 11.2.a) de la LOPD.

La legitimación de las comunicaciones de datos entre Administraciones Públicas a consecuencia de la existencia de una relación jurídica cuyo desarrollo cumplimiento y control requiere la conexión con ficheros de terceros también habilita la creación de registros telemáticos comunes que permita la comunicación de datos entre el registro telemático y la Administración destinataria en quien resida la competencia para la tramitación y resolución de la solicitud [118]. Además, está prevista expresamente la comunicación de datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra —artículo 21.2 de la LOPD—. Hay que resaltar la regulación que hace la LAECSP de los registros electrónicos que deroga las previsiones más restrictivas de la LRJAP y PAC [119]. Así, la LAECSP establece —artículo 24.1— 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. Las Administraciones Públicas podrán, mediante convenios de colaboración, habilitar a sus*

118. Sin embargo, si la comunicación se produce en el ámbito de la misma Administración Pública no debe, a nuestro juicio, entenderse como cesión.

119. La LAECSP deroga el artículo 38.9 de la LRJAP y 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 artículo 38.4 de la LRJAP y 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»*.

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 artículo 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»* —artículo 24.2—.

Inicialmente la LOPD, así como la LORTAD, permitía 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 comunicación 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 [120]. La comunicación de datos entre Administraciones Públicas para funciones o materias distintas exige una habilitación legal expresa o el consentimiento del interesado. Por tanto, no basta con que técnicamente sea posible la comunicación de los ficheros de las distintas Administraciones Públicas, es necesario que sea jurídicamente legítimo. En este punto España tiene un régimen mucho más restrictivo para la Administración electrónica que el resto de países de la Unión Europea [121]. Las comunicaciones de datos entre Administraciones Públicas que se plantean habitualmente son para el ejercicio de competencias distintas —por ejemplo, cesiones de datos desde la Seguridad Social o desde la Agencia Tributaria para la concesión de subvenciones en el ámbito de la educación—. De hecho, habitualmente sólo hay competencias comunes entre diferentes Administraciones territoriales (salud pública de un Ayuntamiento,

120. Cfr. A. TRONCOSO REIGADA: «La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional», *Cuadernos de Derecho Público,* núm. 19-20, 2003, pp. 299-315.

121. La Directiva, que como hemos señalado en otro momento —Introducción a *An approach to data protection in Europe*—, no diferencia la cesión 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»* —artículo 7.e)—.

salud pública de una C.A. 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 es para una finalidad distinta, salvo que haya una habilitación legal—. Así, no es razonable la comunicación generalizada de bases de datos públicas. No es legítimo que un dato personal facilitado por el interesado para una finalidad sea empleado para finalidades distintas y por Administraciones distintas.

En todo caso, la comunicación de datos personales en el marco de la Administración electrónica, especialmente si se hace en virtud de una habilitación legal, tiene que ser respetuosa con el principio de calidad y de finalidad. La LAECSP afirma en la Exposición de Motivos 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 de Datos de Carácter Personal 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»* —apartado 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» —artículo 9— [122]. Por tanto, con anterioridad a la comunicación de datos, es imprescindible analizar la legislación para determinar que los datos requeridos son necesarios y están previstos en la normativa. 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 que reclama. Además, los datos deben ser cancelados por la Administración cesionaria cuando se haya cumplido la finalidad para la cual han sido recabados —artículo 4.5 de la LOPD—.

La Administración electrónica no sólo permite el acceso automatizado sino también la interconexión permanente de bases de datos [123]. Así, la LAECSP

---

122. A esta cuestión también se ha referido el documento ya citado del Grupo del Artículo 29 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».

123. 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. En Italia está en ejecución un proyecto nacional de creación de una

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 —artículo 43— [124]. 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 uno de ellas como, en su caso, la prestación conjunta de servicios a los ciudadanos»* —artículo 4.e)—. En todo caso, hay que tener en cuenta que no es lo mismo el acceso automatizado que la interconexión entre bases de datos ya que el segundo supuesto incrementa el riesgo y supone una mayor injerencia en el derecho fundamental a la protección de datos. Así, mientras que en el acceso automatizado es sencillo que el responsable del fichero lleve a cabo una comprobación individualizada de que la cesión cumple la legislación de protección de datos y, especialmente, de las causas de legitimación para la cesión —que existe el consentimiento del interesado, una habilitación legal, una relación negocial o que sea para competencias semejantes sobre materias comunes— y del principio de calidad, esto es más complejo en el caso de las interconexiones de bases de datos, donde desaparece la supervisión administrativa 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 [125]. Esto obliga a que tanto el responsa-

---

«red de la administración pública unificada», esto es, una red electrónica que conectará a todas las autoridades administrativas del país. Cfr. Documento de trabajo del Grupo de Protección de datos del artículo 29, relativo a la administración en línea, cit.

124. 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 debe seguir su específico régimen jurídico —artículos 33 y 34 de la LOPD—.

125. 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*

ble 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 tanto para el responsable del fichero y cedente como para el cesionario [126].

---

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, 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 una Disposición Adicional Quinta en la Ley Orgánica 4/2000, de 11 de enero, por la que se regulan 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 establecen medidas de seguridad.

126. 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, como más adelante señalaremos, la puesta a disposición de información para otros órganos de la misma o 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. 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 las autoridades 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 se 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 el borrador de Recomendación de la APDCM sobre tratamiento de datos de carácter personal en los servicios de Administración electrónica.

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 obligue a lo establecido en el artículo 12 de la LOPD [127]. 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 artículo 12 de la LOPD [128]. También puede acudirse a la figura del

---

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 servicio 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»*.

127. 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.

128. 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 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.

encargado del tratamiento cumpliendo lo establecido en el artículo 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— [129]. Como ya hemos señalado antes, 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.

3.5. LA SEGURIDAD COMO GARANTÍA DE LA INTEGRIDAD, AUTENTICIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN ADMINISTRATIVA

En quinto lugar, la Administración electrónica tiene que tener en cuenta especialmente el cumplimiento del principio de seguridad. En la medida en que los datos personales 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 —artículo 9 de la LOPD—. Por tanto, mientras el almacenamiento de datos personales en papel no estaba sujeto hasta ahora a unas concretas medidas de seguridad [130], estas medidas de seguridad siempre han existido en el caso de

---

129. 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.

130. El Reglamento de desarrollo de la LOPD contiene ya un conjunto de medidas de seguridad para los ficheros manual-estructurados.

los ficheros informatizados y son de plena aplicación a los tratamientos de datos personales en la Administración electrónica (131). Como hemos señalado anteriormente, las medidas de seguridad dependen sobre todo de la tipología de datos objeto de tratamiento, pudiendo ser de carácter básico, medio o alto (132). Esto es especialmente importante en los procedimientos de Administración Electrónica donde se almacenen datos especialmente protegidos como es el caso de la salud —historias clínicas electrónicas—, de los servicios sociales —historias sociales en soporte electrónico— de la justicia —expedientes judiciales— 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 (133), salvo que exista una

131. Estas medidas de seguridad se encontraban hasta ahora recogidas en el Real Decreto 994/1999, de 11 de junio, y ahora se recogen en el Real Decreto 1720/2007, de 21 de diciembre. 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. Cuando el tratamiento es parcialmente automatizado —o mixto— es necesario implantar las medidas apropiadas a cada tipo de soporte.

132. 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 nivel medio. Con ello queremos decir que, deberán implementarse sobre fichero los dispositivos técnicos que garanticen los niveles de seguridad que especifica el 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 una Infracción a la Universidad de Castilla-La Mancha por un fallo de seguridad que permitió acceder por Internet al fichero con datos de acceso a direcciones web de los trabajadores de la Universidad. A esta cuestión nos hemos referido en la Introducción a *Protección de datos personales para Universidades,* Civitas-APDCM, 2008, p. 27.

133. Así, la participación social implica en ocasiones una valoración política o ideológica. Este 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. Por otra parte, la seguridad de la información tiene que garantizar el carácter secreto del sufragio. Así, a

voluntad de dar a conocer las propias opiniones —como es el caso de la participación en *blogs* o foros de discusión en sitios web de las Administraciones Públicas—.

La seguridad de la información es especialmente importante en el ámbito de la Administración electrónica ya que va encaminada a garantizar la disponibilidad, la autenticidad y la integridad de los datos personales (134). De esta forma, la seguridad permite la conservación de la información 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. No es posible asumir la validez de un documento administrativo si no se encuentra garantizada su autenticidad y su integridad. También es importante la seguridad como garantía de la confidencialidad (135), al evitar que los tratamientos se conviertan en cesiones indiscriminadas de datos personales, permitiendo que sólo accedan a la información las personas autorizadas, evitando los accesos indebidos por par-

---

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 problemas de confianza. Por tanto, las incertidumbres en materia de seguridad de la información son una de las causas de la no introducción del voto electrónico. Sin embargo, sí se pueden utilizar 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», pro manuscrito 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.

134. El Grupo del Artículo 29 en el documento ya citado sobre administración en línea resalta que 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.

135. Por ejemplo, el uso de la red como depositaria 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. Cfr. nuestra Introducción a *Protección de datos en los Servicios Sanitarios Públicos*, cit.

te de terceras personas, especialmente en las comunicaciones realizadas entre los ciudadanos y la Administración y entre las propias Administraciones Públicas [136].

La normativa administrativa ha obligado tradicionalmente a las Administraciones 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 electrónicos, informáticos y telemáticos para la iniciación, tramitación y terminación de los procedimientos administrativos [137]. 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»* —artículo 6.2.l)— 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*

136. Por ello, es especialmente importante que los servicios de Administración electrónica cuenten con adecuados sistemas de identificación y autenticación que acrediten, de manera inequívoca, la identidad del interesado y la autenticidad de los datos y documentos aportados, y deben implantar medidas que permitan al responsable de seguridad llevar a cabo un completo control de los accesos realizados. 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. El artículo 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»*.

137. Así, por ejemplo, el artículo 38.9 de la LRJAP y PAC exigía que los registros telemáticos cumplieran los criterios de disponibilidad, autenticidad, integridad, confidencialidad y conservación de la información. Igualmente, el artículo 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 artículo 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.

medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos» —artículo 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»* —artículo 1.2—. La LAECSP insiste en 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 harán *«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»* —artículo 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 —artículo 4.g)—. Sin embargo, estas medidas de seguridad deben adaptarse especialmente a la tipología de datos sometidos a tratamiento y a su finalidad, como así establece la normativa relativa a las medidas de seguridad de los ficheros informatizados.

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 [(138)] y que resulten adecua-

138. 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 más en las relaciones con la Administración y sólo en el tráfico ordinario de la empresa —límites cuantitativos—. La Ley señala en el artículo 4 que se aplicará al uso de la firma electrónica 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. 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.

dos para *«garantizar la identificación de los participantes, y, en su caso, la autenticidad e integridad de los documentos electrónicos»* —artículo 13.1— [139]. 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 [140], 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 —artículo 13.2 de la LAECSP— [141]. Hay que destacar especialmente que 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.

La LAECSP incide en la importancia de la seguridad de la información dentro de la Administración electrónica [142]. Así, al regular la sede electrónica, señala que

---

139. 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—; 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—.

140. 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. 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 (Finlandia, España, Francia) o de cifrado de datos (Francia, Portugal, España).

141. 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 el establecimiento con ella de comunicaciones seguras. b) Sistemas de firma electrónica para la actuación administrativa automatizada. c) Firma electrónica del personal al servicio de las AAPP. d) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes —artículo 13.3 de la LAECSP—.

142. Igualmente, el artículo 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*

su establecimiento *«conlleva la responsabilidad del titular [de la sede electrónica] respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma»* —artículo 10.1—, un aspecto que también resalta la Exposición de Motivos —apartado VI— (143). 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 —artículo 10.2—. 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»* —artículo 17 de la LAECSP—. Los registros electrónicos también deberán contar *«con las medidas de seguridad necesarias para garantizar su integridad»* —artículo 26.1. Esto se 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»* —artículo 30.3—. Este principio también tiene plena aplicación en el archivo electrónico de documentos, ya que los *«medios o soportes en que se almace-*

---

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».

143. 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 —artículo 8.2.a) de la 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 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 a la que se accedió. 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. A. SÁNCHEZ NAVARRO: «La articulación del derecho a la protección de datos de carácter personal», loc. cit., p. 110.

nan documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados» —artículo 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 —artículo 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»* —artículo 32.2—. También establece que *«deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan»* —artículo 20.3—. Los requerimientos de seguridad también se aplican a las comunicaciones electrónicas (144). 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 —artículo 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 aquellas, de acuerdo con los principios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal»* —artículo 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 —artículo 41—.

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 ga-

144. Un factor de riesgo es la utilización de conexiones electrónicas por Internet y obligada 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 artículo 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 que *«los instrumentos de cifrado que impiden el pirateo de la información transmitida por Internet responden a la obligación del responsable del tratamiento de datos de adoptar medidas adecuadas para proteger los datos personales frente al tratamiento ilícito».*

rantizar 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, mejorando la custodia del almacenamiento y de la remisión de la información en papel que era muy difícil de gestionar (145), cuya confidencialidad dependía, en muchas ocasiones, del cumplimiento del deber de secreto por parte de los empleados públicos —artículo 10 de la LOPD— (146). 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 (147).

3.6. EL EJERCICIO DE LOS DERECHOS Y LA ACTIVIDAD DE LAS AUTORIDADES DE CONTROL

En sexto lugar, la Administración electrónica debe garantizar los derechos de acceso, oposición, rectificación y cancelación del interesado sobre sus datos

145. 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.

146. 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»* —artículo 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.

147. 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 contraseñas, 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.

personales almacenados en los distintos procedimientos administrativos [148]. No obstante, en este caso 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 telemáticos [149]. El derecho de acceso a los datos personales del artículo 15 LOPD es distinto al derecho a conocer el estado de tramitación de los procedimientos en los que se sea interesado y a obtener copias de documentos contenidos en ellos —artículo 35.a) de la LRJAP y PAC—, ya que el primero implica una información sobre los datos objeto de tratamiento, la finalidad del mismo, el origen de los datos y las posible comunicaciones a terceras personas [150], lo que no incluye el segundo que se limita a ofrecer una información sobre los actos de trámite en el marco de un procedimiento administrativo no concluido. La LAECSP proclama el derecho a *«conocer por medios electrónicos el estado de tramitación de los procedimientos en los*

148. En la Resolución 400/2006 —ya citada— de la Agencia Española se 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. 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), obliga 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 Públicas, Jueces y Tribunales.

149. Hemos señalado anteriormente que la Agencia de Protección de Datos de la Comunidad de Madrid ha impulsado una aplicación de ejercicio telemático de derechos de protección de datos (DEPD) que facilita a los ciudadanos el ejercicio de los derechos de acceso, rectificación y cancelación ante el responsable del 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.

150. Artículo 15 de la LOPD, artículo 12 del Real Decreto 1332/1994, de 20 de junio —ya derogado— y artículo 27 del Reglamento de desarrollo de la LOPD.

que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquéllos» —artículo 6.2.d)—. También señala que en *«[e]n los procedimientos administrativos gestionados en 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»* —artículo 37—. Lógicamente, el derecho a conocer por medios electrónicos el estado de tramitación de un expediente en el que se tenga la condición de interesado supone también la cesión de datos de otras personas que se encuentran en los documentos electrónicos y que se llevaría a cabo sin el consentimiento del interesado al existir en este punto una clara habilitación legal —artículo 11.2.a) de la LOPD—. La LAECSP regula de manera separada el derecho a *«obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado»* —artículo 6.2.e)—. No le corresponde a la LAECSP regular el derecho de acceso a los propios datos personales sometidos a tratamiento en el ámbito de la Administración electrónica. No obstante, sí podía haber establecido expresamente la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición en el marco de la Administración electrónica [151].

151. Cualquier servicio de administración electrónica que proceda al tratamiento de datos de carácter personal está obligado a facilitar al interesado el ejercicio de los derechos de protección de datos personales. Por ello, estos servicios deben incorporar las herramientas necesarias para atender estas solicitudes de ejercicio de derechos, implantando 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-. En la medida de lo posible, el ejercicio del derecho de acceso deberá poder 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 de-

Por último 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 de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad»* —artículo 13.1 de la LOPD—. 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»* —artículo 13.2—. Si bien las decisiones administrativas no se encuentran basadas en la personalidad, sí lo pueden estar en virtud de las características [152]. 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 esté autorizada por una norma de rango legal que establezca medidas que garanticen el interés legítimo del interesado —artículo 36.2.b)—. 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 —artículo 13.3 de la LOPD—. Hay que mencionar que la LAECSP prevé la utilización de medios electrónicos en la tramitación del procedimiento administrativo —artículos 35 a 39— y establece la existencia de actuaciones administrativas automatizadas que son producidas por un sistema de información adecuadamente programado sin necesidad de

---

sea 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. Sobre esta cuestión, cfr. el borrador de Recomendación de la APDCM sobre tratamiento de datos de carácter personal en servicios de Administración electrónica.

152. *«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. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado»* —artículo 13.3 y 4—. Esta es una cuestión bastante importante en el ámbito de los servicios sociales. Cfr. nuestra Introducción a *Protección de datos personales en los Servicios Sociales Públicos,* cit.

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)— [153]. Como única garantía se 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»* —artículo 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 el cumplimiento de los principios de protección de datos personales y de los derechos también en el ámbito de la Administración electrónica —artículos 37 y 41 de la LOPD—. 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»* —artículo 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 —artículo 6.2.i)—, sus competencias

153. El artículo 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 recursos que puedan interponerse».* Los programas y aplicaciones electrónicos, informáticos y telemáticos 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 artículo 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».*

afectan a las Agencias de Protección de Datos, especialmente a las de la Agencia Española de Protección de Datos. Hay que señalar que el defensor del usuario, si bien desarrolla 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 (154).

154. Esta cuestión la hemos analizado en «La Administración Independiente en la Comunidad de Madrid», en E. ÁLVAREZ CONDE y R. PLAZA DE DIEGO: *Derecho Público y Administración de la Comunidad de Madrid,* Tirant lo Blanch-IMAP, Madrid, 2008, pp. 1081-1116.