

E-Administración, identificación del ciudadano y protección de datos personales en la Unión Europea: ¿una ecuación posible?

(A propósito del Documento Nacional de Identidad electrónico en España)

Julián Valero Torrijos

Professor de Dret Administratiu. Universitat de Murcia

Director del curs a distància *La protección de los datos de carácter personal*, que organitza la Facultat de Dret de la Universitat de Múrcia.

Francisco Javier Sanz Larruga

Professor de Dret Administratiu. Universitat de la Corunya

(Comunicación presentada en el XXVI Congreso Internacional de Ciencias Administrativas, celebrado en Seúl (Corea del Sur), del 14 al 18 de julio de 2004).

1.- La firma electrónica: una exigencia técnica para la prestación telemática de los servicios públicos

Tal y como ha destacado la Comisión Europea en su Comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones, sobre el papel de la Administración electrónica en el futuro de Europa, es necesario precisar que, si bien la utilización de las tecnologías de la información y la comunicación en la actividad administrativa constituye una herramienta imprescindible en la tarea modernizadora que exige la eficacia que aquella debe perseguir, no por ello pueden minusvalorarse otras medidas que necesariamente deben adoptarse¹. En efecto, resulta imprescindible la puesta en marcha de reformas organizativas tendentes a garantizar la efectiva funcionalidad de los medios técnicos empleados, la oferta de un programa de formación específico para el personal administrativo y, desde una perspectiva estrictamente jurídica, la adopción de aquellas reformas necesarias para adecuar el marco jurídico reguladora de la actividad administrativa a las singularidades que conllevan el uso de los medios informáticos y telemáticos.

Uno de los presupuestos básicos para el efectivo desarrollo de la e-Administración desde la perspectiva jurídica consiste en que se garantice de forma razonablemente segura la identidad de los ciudadanos en las relaciones telemáticas que entablen con las entidades públicas ya que, si bien es cierto que muchas actuaciones pueden realizarse anónimamente, la mayor parte de las que ofrecen un valor añadido precisan de tal requisito. Así sucede, por ejemplo, con la presentación de solicitudes y documentos, el acceso a la información administrativa en el seno de un procedimiento administrativo, la participación en el mismo o, sin ánimo exhaustivo, la recepción de notificaciones. Así pues, a salvo del acceso a información administrativa de carácter genérico a través de sitios web o previa petición formal, la mayor parte de las relaciones con la Administración Pública precisan de la previa comprobación de la identidad del ciudadano, hasta el punto de que la falta de las oportunas medidas de seguridad en estas actuaciones puede considerarse una vulneración de las normas sobre protección de datos personales.

La solución técnica sobre la que se han desarrollado hasta la fecha las iniciativas de e-Administración para cumplir esta exigencia ha sido la firma digital que, siempre que se cumplan determinados requisitos, puede considerarse equivalente a la firma manuscrita. A este respecto, el artículo 5 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, exige a los Estados miembros que adopten las medidas normativas oportunas para que "la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma [...] satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel"². Asimismo, este instrumento permite garantizar de forma razonablemente segura tanto la integridad y autenticidad de los documentos y las declaraciones de voluntad que se remitan telemáticamente, de manera que su uso por parte de las entidades públicas también resulta decisivo desde el punto de vista de la seguridad jurídica de los ciudadanos.

2.- El documento de identidad electrónico: una oportunidad para la generalización de la firma electrónica

A fin de dar respuesta a las necesidades específicas de la firma electrónica en las Administraciones Públicas diversos países europeos han puesto en marcha iniciativas dirigidas a la implantación de un documento de identidad electrónico basado en la tecnología de la firma electrónica³. Dado que el documento de identidad, con independencia de su soporte físico o digital, constituye un elemento indispensable para la identificación de los ciudadanos en aquellos países donde se encuentra establecido, su expedición tiene carácter obligatorio y, en consecuencia, se obtiene de forma gratuita a salvo del cobro de una tasa para asumir los gastos que conlleva su expedición.

En este sentido, en cumplimiento de la citada normativa europea se ha dictado en España la Ley 59/2003, de 19 de diciembre, sobre firma electrónica, una de cuyas principales novedades consiste en la creación de un documento nacional de identidad electrónico "que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos", de manera que todas las personas físicas o jurídicas, públicas o privadas, están obligadas legalmente a reconocer su eficacia "para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos"⁴.

Se trata de una medida que, debido al carácter obligatorio de este documento identificativo, permitirá que todos los ciudadanos españoles dispongan a medio plazo de un instrumento para identificarse en sus relaciones telemáticas y firmar los documentos en soporte digital con las debidas garantías técnicas y jurídicas. Nos encontramos, por tanto, ante una decisión de gran relevancia para el desarrollo de la e-Administración ya, al margen de aquellos supuestos que no requieran la identificación fidedigna de los ciudadanos, un gran número de actuaciones telemáticas ante la Administración Pública requieren inexcusablemente que sean realizadas por el propio interesado o su representante. Pues

bien, si partimos de que estos inconvenientes quedan en gran medida con el empleo de la firma electrónica, el hecho de que todos los ciudadanos dispongan de un certificado digital gratuito constituye sin duda un avance decisivo para la implementación de nuevos servicios telemáticos que podrán ser utilizados por un mayor número de ciudadanos y, en consecuencia, las inversiones necesarias para su puesta en marcha resultarán más provechosas.

Ahora bien, no por ello puede dejar de advertirse sobre algunos importantes problemas jurídicos que esta previsión supone desde una perspectiva europea, tanto por lo que se refiere a algunos de los principios en que se sustenta la normativa reguladora de la firma electrónica como, de forma más preocupante, a las disposiciones encaminadas a la protección de los datos de carácter personal.

3.- La incidencia del documento de identidad electrónico sobre el principio de libre competencia en la prestación de servicios de certificación

Una de las principales características de la regulación que contiene la Directiva 1999/93/CE es la práctica inexistencia de una regulación específica para la prestación de servicios de certificación en el sector público, de manera que, a salvo de previsión en contrario, la normativa general resulta igualmente aplicable en el ámbito administrativo. Únicamente, en el artículo 3.7 se habilita a los Estados miembros en orden al establecimiento de prescripciones adicionales que, en todo caso, habrán de ser objetivas, transparentes, proporcionadas y no discriminatorias, debiendo limitarse a las características específicas de la aplicación de que se trate. Así pues, no existe base normativa suficiente en la citada Directiva para impedir que los servicios de certificación sean prestados por sujetos privados en las relaciones de los ciudadanos con las Administraciones Públicas, a pesar de que en algunos Estados -singularmente es el caso español- tal función ha correspondido tradicionalmente a los poderes públicos mediante la expedición de un documento único de identificación obligatorio, por lo que la firma electrónica viene a establecer un sistema dual en razón de la tecnología utilizada.

Al margen de las críticas que pueden formularse a la normativa europea al no haber contemplado la especificidad de algunos Estados a este respecto -decisión sin duda justificada por la heterogeneidad de los sistemas de identificación en cada uno de los países que integran la Unión Europea y, sobre todo, por la naturaleza jurídico-privada de las razones que justificaron la aprobación de la Directiva 1999/93/CE, fundamentalmente el impulso del comercio electrónico-, lo cierto es que sus previsiones han de ser aplicadas a las relaciones que entablen los ciudadanos con las Administraciones Públicas y, en consecuencia, resulta necesario realizar una labor interpretativa de las mismas que tenga en cuenta esta singularidad.

Por una parte, es necesario recordar que la normativa europea se basa en la libre prestación de servicios de certificación, de manera que los ciudadanos podrían en principio utilizar los certificados expedidos por cualquier sujeto público o privado siempre que reúnan los requisitos técnicos en que se basa la equiparación de la firma electrónica con la manuscrita. En consecuencia, no resulta admisible que las disposiciones reguladoras de los

distintos servicios y actuaciones que pueden llevarse a cabo telemáticamente exijan imperativamente y de forma exclusiva la intervención de un determinado prestador de servicios de certificación, monopolio que suele reservarse a una entidad pública. Ciertamente, la singularidad propia de la actividad que llevan a cabo las Administraciones Públicas puede justificar la exigencia de ciertas condiciones específicas, pero las mismas han de fijarse con carácter general para todos los prestadores y han de respetar las condiciones anteriormente enumeradas: objetividad, transparencia, proporcionalidad y no discriminación. En consecuencia, siempre que se parta de una determinada calidad técnica - en concreto, que sean reconocidos y estén basados en un dispositivo seguro-, cualquier opción monopolística que impidiera al ciudadano el uso de los certificados expedidos por un prestador distinto del indicado por la Administración Pública en cuestión debe reputarse contraria a la Directiva 1999/93/CE al ser discriminatoria.

Por otra parte, la obligatoriedad de que todos los ciudadanos dispongan de un documento de identificación electrónico y, consiguientemente, puedan utilizar los dispositivos de firma electrónica que contiene gratuitamente puede contravenir igualmente la normativa europea. En efecto, si como sucede en el caso español cualquier sujeto está obligado a aceptar la eficacia jurídica del documento de identidad electrónico, ¿qué ciudadano puede estar interesado pagar por utilizar en sus relaciones con las Administraciones Públicas los certificados expedidos por un prestador privado cuando dicho servicio lo obtiene gratuitamente? En concreto, se estaría incumpliendo lo dispuesto en el artículo 4.2 de la Directiva 1999/93/CE puesto que, en definitiva, se estaría perturbando la libre circulación de los productos de firma electrónica en la medida que los impulsados desde el sector privado competirían en condiciones económicas desfavorables y, por lo tanto, su papel se limitaría a ofrecer servicios de valor añadido a la mera identificación.

Ciertamente, nos encontramos ante un problema de enorme complejidad en la medida que supone enfrentar, de un lado, los principios esenciales en que se basa la normativa comunitaria y, de otro, la tradición de algunos Estados en virtud de la cual la identificación fehaciente de los ciudadanos ante las Administraciones Públicas se encuentra reservada a las autoridades públicas. Parece inevitable reclamar una regulación más flexible a nivel europeo que tenga en cuenta estas circunstancias más allá de la pretensión de impulsar el comercio electrónico.

4.- El elemento territorial en la Unión Europea: una complicación añadida para el desarrollo de la e-Administración

La exigencia de la libre prestación de servicios de certificación en la Unión Europea presenta una especial dimensión problemática desde el punto de vista territorial y, singularmente, en razón de la diversidad lingüística existente en los distintos Estados, de manera que la libre circulación de los certificados puede encontrarse con un serio obstáculo por lo que se refiere a la comprensión de los atributos que contiene y que, en definitiva, son los que permiten a la autoridad administrativa con la que se relaciona el ciudadano constatar su identidad y comprobar los datos a que se refieren dichos atributos.

Se trata, sin duda, de un problema de gran trascendencia práctica en orden al efectivo desarrollo de la e-Administración, tanto desde la perspectiva europea como, sobre todo y de , desde el punto de vista de las relaciones entre los ciudadanos y otras Administraciones Públicas distintas de las integradas en su Estado de origen. En efecto, por una parte, las relaciones directas con las autoridades integradas en la organización administrativa de la Unión Europea se irán incrementado conforme se articulen vías telemáticas de comunicación⁵, de manera que si resulta necesaria la identificación del interesado habrá de exigirse la utilización de firma digital que, como no puede ser de otra manera, deberá basarse en los certificados expedidos por el prestador de servicios elegido por el ciudadano siempre que se respeten los requisitos técnicos y jurídicos fijados por la normativa europea.

Incluso, en los últimos años puede advertirse un notable incremento de la circulación de personas físicas y entidades entre los diversos Estados que forman parte de la Unión Europea, de modo que con mayor frecuencia irá presentándose el supuesto de que dichos sujetos deban relacionarse con entidades públicas que no pertenezcan a su Estado de origen. En este caso, por aplicación de los principios en que se basa la Directiva 1999/93/CE y, en concreto, teniendo en cuenta la libre prestación de los servicios de certificación, la Administración Pública se encuentra obligada a admitir la identificación del ciudadano basada en los certificados expedidos por prestadores establecidos en un Estado distinto, lo que sin duda puede llegar a ser un problema cuando la lengua en que se encuentren redactados los correspondientes atributos no se encuentre entre las más comunes. No resulta extraño, por tanto, que el problema de la interoperabilidad de las firmas electrónicas constituya una de las principales preocupaciones de las autoridades europeas en la medida que puede llegar a convertirse en un obstáculo para el desarrollo efectivo de servicios públicos paneuropeos por vía telemática⁶.

La solución a este concreto problema pasa necesariamente por una flexible interpretación de la normativa vigente adaptada a la realidad sobre la que ha de proyectarse. Según lo previsto en el artículo 3.7 de la Directiva 1999/93, el uso de la firma electrónica en el ámbito público puede encontrarse supeditado a prescripciones adicionales por parte de los Estados para adaptarse a las singularidades de la aplicación o programa que se deba utilizar, exigencia que puede constituir un obstáculo para la prestación de servicios transfronterizos al ciudadano si dicha facultad se concibe con excesiva amplitud. Más aún, si bien la Directiva antes citada garantiza la existencia de una mínima armonización en cuanto a la eficacia de la firma digital, lo cierto es que en algunos casos las legislaciones nacionales han establecido una presunción de equiparación cuando el prestador y los certificados reúnan determinados requisitos, por lo que cabría plantearse el supuesto de que los servicios ofrecidos por un prestador extranjero no reunieran alguna de dichas exigencias a pesar de ofrecer una seguridad incluso mayor desde el punto de vista técnico y, en consecuencia, sus productos no tuvieran reconocida en ese otro Estado una eficacia proporcionada a su calidad técnica.

En consecuencia, partiendo de los principios en que se fundamenta la Directiva 1999/93/CE sobre firma electrónica, la fijación de estos requisitos adicionales por parte de los Estados únicamente puede justificarse desde una perspectiva técnica pues, de lo contrario, se vulneraría el espíritu de la normativa europea en la materia. Por lo que se refiere concretamente al problema de la lengua en que se encuentren redactados los

atributos de los certificados, los inconvenientes únicamente pueden surgir respecto de aquellos datos que no se refieran al nombre y apellidos del interesado y, adicionalmente, no tengan carácter numérico puesto que, en ambos casos, parece irrelevante la lengua en que se encuentren redactados. Así pues, por lo que se refiere a la cuestión lingüística, sólo en aquellos procedimientos en que fuera imprescindible tener en cuenta atributos distintos de los anteriores a fines estrictamente identificativos estaría justificado que los Estados fijaran requisitos adicionales y, en consecuencia, se podría exigir una previa acreditación de los prestadores y sus certificados por parte de las autoridades estatales. En última instancia, de no admitirse esta interpretación, se estaría vulnerando tanto la prohibición del artículo 3.7 de la Directiva 1999/93/CE por cuanto tal medida constituiría un obstáculo a los servicios transfronterizos desde la perspectiva del ciudadano. Adicionalmente, se estaría igualmente contraviniendo el artículo 4.1 de la citada Directiva ya que, en definitiva, tales medidas restringirían la prestación de servicios de certificación que procedan de otro Estado miembro.

Por último, la dimensión supranacional de la Unión Europea plantea asimismo relevantes cuestiones en relación con la protección de los datos de carácter personal, fundamentalmente como consecuencia de la inexistencia de una regulación específica de su utilización por parte de las entidades públicas en la Directiva 1995/46/CE, aspecto que se analizará pormenorizadamente en el siguiente epígrafe.

5.- Una problemática de singular importancia: la protección de los datos personales ante la prestación de servicios públicos transnacionales

5.1. Planteamientos generales

Al margen de los inconvenientes relativos a la firma electrónica como consecuencia de la tensión entre la libre prestación de servicios de certificación y el carácter supraestatal de las relaciones que se entablan entre las entidades públicas y los ciudadanos, uno de los principales retos que han de asumirse para garantizar la eficacia de sus derechos como consecuencia de la utilización de medios informáticos y telemáticos es la adaptación de la normativa reguladora de la protección de los datos de carácter personal.

Como ha destacado el Grupo del artículo 29⁷, el éxito de ciertos proyectos sobre e-Administración depende en gran medida de cuestiones relacionadas con la protección de los datos personales, tal y como sucede singularmente con 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 públicos. Más allá de los problemas generales que para la salvaguarda de este derecho supone el uso de medios tecnológicos avanzados desde una perspectiva interna y que, en última instancia, puede considerarse un auténtico *caballo de Troya* para la consolidación de la e-Administración, lo cierto es que la proyección europea de los servicios públicos constituye un riesgo añadido en dicha trascendental tarea en la medida que resulta necesario que los datos personales de los ciudadanos circulen más allá de las limitaciones geográficas propias de los Estados que integran la Unión Europea.

En efecto, para hacer realidad la prestación de servicios públicos electrónicos más allá de las fronteras de cada Estado miembro de la Unión Europea es necesario que las diversas entidades públicas implicadas compartan los datos personales que tienen en su poder, para lo cual sería deseable que desde la Unión Europea se adoptara un marco normativo específico donde se fijen los requisitos, condiciones y límites en que tales cesiones informativas han de llevarse a cabo sin merma de la protección jurídica de los ciudadanos. Esta necesidad adquiere una mayor trascendencia si observamos que la Directiva 1995/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, contiene simplemente un régimen general en el que se autorizan determinadas limitaciones en el ámbito público que, en última instancia, debe ser concretadas por cada Estado⁸.

En ejercicio de esta habilitación, los poderes públicos estatales han llevado a cabo un desarrollo normativo heterogéneo que puede dificultar la transferencia de los datos personales necesarios para la tramitación telemática de los procedimientos administrativos, especialmente cuando se trate de actuaciones susceptibles de producir efectos desfavorables para los ciudadanos y, de modo muy singular, las de carácter sancionador. En este sentido, aunque el Plan de Acción e-Europe 2005 reconoce al programa IDA como el instrumento operativo clave para la prestación de servicios paneuropeos de Administración electrónica, lo cierto es que el camino por recorrer todavía es considerable a la vista de las limitaciones que presenta dicha iniciativa⁹, tal y como se analizará posteriormente en relación con las cesiones interadministrativas.

5.2. Análisis de las principales cuestiones que suscita la protección de los datos personales en la prestación de servicios transnacionales por vía telemática

En primer lugar, es preciso destacar que la insuficiencia y falta de adaptación del actual marco normativo europeo en relación con el presupuesto de hecho sobre el que ha de construirse la e-Administración en la Unión Europea, al menos desde la perspectiva de la regulación general contenida en la Directiva 1995/46/CE y con la salvedad de las disposiciones específicas existentes para determinados sectores, singularmente los relacionados con la seguridad pública. En efecto, a pesar de que la implementación de servicios transnacionales conlleva irremediamente la cesión de datos personales entre diversas Administraciones Públicas, lo cierto es que la citada Directiva sólo se ha preocupado de autorizar el establecimiento de excepciones por parte de los Estados a las reglas generales que ella misma fija, de manera que no existe realmente un régimen uniformizado concebido específicamente para la protección de los datos personales en poder del sector público con independencia del Estado al que nos refiramos. Más aún, puede afirmarse que existe un nivel de protección ciertamente variable en razón del carácter más o menos garantista de la regulación estatal de que se trate, no sólo por lo que se refiere a las disposiciones propias del sector público sino, más aún, a los principios y reglas generales.

Teniendo en cuenta este presupuesto, resulta necesario determinar la legislación estatal aplicable cuando resulte necesaria la cesión de los datos personales entre Administraciones Públicas sometidas a regulaciones estatales diversas o, en su caso, cuando se proceda a la

creación de bases de datos comunes accesibles por vía telemática. En relación con estos supuestos es necesario advertir la manifiesta falta de adecuación de la regla general sobre el Derecho nacional aplicable que se contiene en el artículo 4 de la Directiva 1995/46/CE, donde se parte del sometimiento a las reglas propias del Estado donde se localice el establecimiento del responsable del tratamiento, de modo que si éste se encontrara establecido en varios Estados deberá adaptar su actividad a las disposiciones de cada uno de ellos. Se trata, por tanto, de una regla inviable para las Administraciones Públicas por cuanto, dada la vinculación del poder público con la soberanía estatal, sus establecimientos sólo se encuentran en un Estado y, dado que resulta necesario compartir datos personales para la prestación de este tipo de servicios -transnacionales-, necesariamente nos encontramos ante dos entidades públicas pertenecientes a Estados diferentes y con su propia personalidad jurídica. Así pues, o ambas Administraciones Públicas se comprometen a respetar recíprocamente su normativa o, desde una consideración jurídica, la actuación administrativa basada en la cesión de los datos no podría llevarse a cabo a menos que se cuente con el consentimiento de los afectados, requisito de difícil cumplimiento en los procedimientos susceptibles de producir actos desfavorables como los de naturaleza sancionadora.

Así, cabría imaginar que un determinado Estado dispusiera de una regulación flexible en orden a permitir la utilización de la información en poder de sus entidades públicas por parte del sector privado. Si se admite la cesión de los datos personales sin un nivel equiparable de garantía al del Estado de origen se llegaría al absurdo de que, en última instancia, los mismos podrían acabar en poder de una empresa o particular del mismo país de donde provienen donde, por aplicación de sus propias normas, tal disposición sería inviable. Más aún, en el caso de las cesiones de datos entre Administraciones Públicas, tales operaciones, si bien justificadas en base al cumplimiento de fines de interés público, sólo podrían admitirse sin consentimiento del afectado cuando la comunicación estuviera amparada en el ordenamiento jurídico del Estado cedente y, adicionalmente, su uso fuera legítimo en las condiciones establecidas por las normas propias del cesionario. Dadas las dificultades que supone la prestación de servicios públicos con estos obstáculos, no puede más que concluirse la necesidad de adoptar un régimen jurídico más preciso y detallado que el propio de la Directiva 1995/46/CE que, en definitiva, se limita a establecer genéricas excepciones que habrán de ser precisadas por cada uno de los Estados miembros con arreglo a las particularidades de su sistema jurídico.

El problema se complica sustancialmente si atendemos a la configuración del derecho a la protección de los datos personales en algunos países como España. En efecto, según dispone el artículo 18.4 de la Constitución Española de 1978, nos encontramos ante un *derecho fundamental*, calificación que tiene gran relevancia a los efectos de su tutela: su contenido esencial en un sentido positivo y negativo -esto es, las facultades y obligaciones del titular- ha de ser precisado mediante una norma con rango de ley, si bien el legislador no dispone de un ilimitado margen en su configuración puesto que, como ha advertido el Tribunal Constitucional, ya que "debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora" pues, de lo contrario, se estarían vulnerando las exigencias de seguridad jurídica constitucionalmente garantizadas, tal y como sucede singularmente con la utilización de la expresión "interés público" para limitar el ejercicio de los derechos de acceso, cancelación y rectificación por parte de los

afectados¹⁰. Teniendo en cuenta esta exigencia, cuando los datos personales de un ciudadano hubieran sido cedidos por la Administración española a la de otro Estado, debería articularse un nivel de garantía equivalente tanto formal como materialmente pues, de lo contrario, no parece admisible que pueda tener lugar la cesión sin el consentimiento del titular de los datos, conclusión que, sin duda, constituye un obstáculo de gran relevancia para el desarrollo de servicios públicos telemáticos que, en última instancia, se basan en la facilidad -técnica y jurídica- para el intercambio de la información necesaria para el ejercicio de las competencias administrativas.

6.- A modo de conclusión

Así pues, a la vista de las razones que se han expuesto, podemos afirmar que resulta imprescindible y urgente la adaptación del marco jurídico vigente en la Unión Europea en que se sustenta la e-Administración. En efecto, por lo que se refiere a la firma digital, resulta imprescindible establecer disposiciones específicas que tengan en cuenta las particularidades de la prestación de servicios de certificación en el ámbito de las Administraciones Públicas, de manera que el eventual requerimiento de una autorización administrativa no se convierta en una vulneración injustificada del principio de libre prestación de tales servicios no sólo por las entidades privadas sino, también y principalmente, por las de naturaleza pública. Por lo que se refiere a la protección de los datos personales, ha quedado evidenciada la inexistencia de una regulación a nivel de la Unión que permita garantizar la protección de este derecho en un nivel adecuado y, en definitiva, conjugarla con la satisfacción de los intereses públicos. Es necesario reclamar, por tanto, que la excesiva generalidad de la Directiva 1995/46/CE sea concretada más allá de regulaciones sectoriales en una regulación común suficientemente detallada que se enfrente decididamente con la singularidad del sector público, debiendo reclamarse en todo caso un papel protagonista del Parlamento Europeo que colme los requerimientos democráticos imprescindibles a la hora de tutelar este derecho.

Notas

1. COM(2003) 567 final, apartados 3 y 4.2.7.
2. Por lo que se refiere a los requisitos técnicos a que se refiere el precepto transcrito, el Anexo I de la Directiva 1999/93/CE se refiere a los que han de contener los certificados reconocidos, el Anexo II a los que han de respetar los prestadores de servicios que expidan dichos certificados y, finalmente, el Anexo III contiene las exigencias técnicas a que han de adaptarse los dispositivos seguros de creación de firma.
3. Una visión de conjunto de los sistemas obligatorios de identificación de los ciudadanos existentes en los distintos Estados de la Unión Europea, ya generales ya sectoriales, se contiene en el Documento sobre la Administración en línea, adoptado el 8 de mayo de 2003 por el Grupo de trabajo creado al amparo del artículo 29 de la Directiva 95/46/CE, cuyo texto se encuentra accesible a través de Internet en .

4. Artículo 15 de la Ley 59/2003, de 19 de diciembre (Boletín Oficial del Estado núm. 304 de 20 de diciembre). El texto de la misma se encuentra accesible a través de Internet en <http://www.boe.es/g/es/boe/dias/2003-12-20/seccion1.php>.

5. Un ejemplo ciertamente paradigmático sería la presentación de quejas y peticiones ante el Defensor del Pueblo europeo. Aunque según se dispone en su sitio web oficial <http://www.euro-ombudsman.eu.int> es posible contactar con dicha autoridad a través de su dirección de correo electrónico -euro-ombudsman@europarl.eu.int-, todavía no se contempla la necesidad de acreditar de forma fidedigna la identidad del solicitante que, de utilizarse esta vía telemática, debería realizarse a través de la firma electrónica. Quizás las dificultades a las que nos referimos en este trabajo se encuentren en la base de esta insuficiente seguridad técnica y jurídica.

6. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. El papel de la administración electrónica en el futuro de Europa, COM(2003) 567 final, apartado 4.2.2.

7. Grupo de trabajo creado al amparo del artículo 29 de la Directiva 95/46/CE, cuyo *Documento sobre la Administración en línea*, adoptado el 8 de mayo de 2003, se encuentra accesible a través de Internet en http://europa.eu.int/comm/internal_market/privacy/workinggroup_en.htm.

8. A estos efectos, cabe destacar el artículo 7, donde se autoriza el tratamiento de los datos sin consentimiento cuando "es 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"; la prohibición del tratamiento de los denominados *datos sensibles*, salvo que por motivos de interés público importante los Estados excepcionen esta regla; o, fundamentalmente, las excepciones y limitaciones a los derechos del titular cuando concurren las razones previstas en el artículo 13.

9. El marco jurídico general de esta iniciativa se contiene en la Decisión 1719/1999/CE del Parlamento Europeo y del Consejo, de 12 de julio de 1999, sobre un conjunto de orientaciones, entre las que figura la identificación de los proyectos de interés común, relativo a redes transeuropeas destinadas al intercambio electrónico de datos entre administraciones (IDA), texto accesible a través de Internet en <http://europa.eu.int/ISPO/ida>.

10. Sentencia 292/2000, de 30 de noviembre, accesible a través de Internet en el sitio web del Tribunal Constitucional <http://www.tribunalconstitucional.es/STC2000/STC2000-292.htm>.