La gestión electrónica de la identidad y de la firma electrónica en el intercambio electrónico de datos entre Administraciones Públicas

Ignacio Alamillo, Erika Henao Hoyos*

Abstract: A efectos del presente artículo resulta de especial relevancia el análisis de tres de los derechos consagrados y los correspondientes modelos técnico-jurídicos para su aplicación: el derecho a obtener los medios de identificación electrónica necesarios , el derecho a la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas , y el derecho a no aportar los datos y documentos que obren en poder de las Administraciones Públicas .

I. El panorama actual

Es evidente que asistimos en la actualidad a un momento en el cual las Administraciones Públicas se encuentran inmersas en un proceso de digitalización de sus procedimientos, cuestión de la que se derivan consecuencias de diversa índole, tanto desde la perspectiva del administrado como de la perspectiva de la misma Administración.

La utilización de las nuevas tecnologías en la actividad administrativa supone un cambio de paradigma de gran trascendencia, en primer lugar, para el ciudadano. La implantación de la Administración electrónica ofrece la posibilidad de ejercer vía online, durante las 24 horas del día, todos los días del año y sin limitaciones geográficas, el catálogo de derechos del que tradicionalmente ha sido titular, según la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante LRJAP-PAC). Sin ánimo de ser exhaustivos: el derecho al conocimiento sobre el estado de la tramitación de los procedimientos en los que ostente la calidad de interesado, el derecho a la obtención de copias electrónicas de los documentos que obren en el expediente, el derecho a formular alegaciones y a aportar documentos en cualquier fase del procedimiento, son algunos de los mencionados derechos.

Y es importante catalogar de “tradicionales” los derechos a los que se acaba de hacer alusión, ya que con la aparición de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (en adelante LAECSP) se

configuran nuevos derechos que desbordan la tradicional lógica del derecho administrativo.

Más concretamente, el artículo 1 de la citada ley reconoce el derecho de los ciudadanos a relacionarse por medios electrónicos con las Administraciones Públicas[1]. Éste se erige, sin duda, en la pieza angular de la ley, ya que plantear el uso de las nuevas tecnologías por parte del administrado en términos de derecho y no de mera posibilidad[2] constituye un cambio de orientación radical del concepto de Administración.

El artículo 6 es el encargado de consagrar los derechos que le asisten a los ciudadanos en su relación electrónica con las Administraciones Públicas. En primer lugar, el legislador ha destacado como fundamental el derecho a tener una participación activa en el procedimiento administrativo, esto quiere decir que el ciudadano tiene derecho a: "obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos"[3].

En el numeral dos del mismo artículo son consagrados los derechos que tiene el ciudadano en relación con la utilización de los medios electrónicos en la actividad administrativa. Algunos de ellos son el derecho a elegir, siempre y cuando se encuentre disponible, el canal a través del cual se relacionará con las Administraciones Públicas; el derecho a la igualdad en el acceso electrónico a los servicios de las Administraciones Pública; el derecho a obtener copias electrónicas de los documentos electrónicos o el derecho a la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente, etc.

A efectos del presente artículo resulta de especial relevancia el análisis de tres de los derechos consagrados y los correspondientes modelos técnico-jurídicos para su aplicación: el derecho a obtener los medios de identificación electrónica necesarios[4], el derecho a la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas[5], y el derecho a no aportar los datos y documentos que obren en poder de las Administraciones Públicas[6].

II. La identidad y la firma electrónica

En primer lugar, dedicaremos algunas líneas al derecho que consideramos crucial para la implementación de la Administración electrónica. Es claro que el derecho del ciudadano a relacionarse por medios electrónicos con las Administraciones Públicas es el derecho que mayor relevancia tiene de todos los consagrados en la LAECSP. En nuestra opinión, es innegable la revolución que supone el reconocimiento de un derecho como éste; sin embargo, consideramos, bajo la perspectiva de un análisis global del ordenamiento jurídico, que existe un derecho que le antecede y sin el cual la administración electrónica no sería más que una quimera: el derecho a la identidad electrónica – que también podemos denominar "derecho a la acreditación electrónica

de la identidad" – que se manifiesta y desarrolla en el derecho al uso de la firma electrónica.

Aunque este derecho, evidentemente, no tiene un carácter de fundamental en nuestro ordenamiento jurídico[7] y, en consecuencia, no goza de un sistema de garantía reforzado ni para su protección ni para su desarrollo legislativo, podríamos afirmar que la puesta en marcha de todo proyecto de "Administración electrónica" implica necesariamente el establecimiento y la ejecución de una política pública que tenga por objetivo proporcionar al ciudadano los medios de identificación necesarios, como condición necesaria (aunque no suficiente) para la viabilidad del proyecto.

En este sentido, nos encontramos con que el ciudadano que no pueda obtener o emplear dichos medios de identidad puede considerarse hoy día como un ciudadano discriminado, al no poder ejercer su derecho a la comunicación electrónica con la Administración, situación que genera una vulneración del derecho fundamental a la igualdad[8]. Y el respeto de los derechos fundamentales implica, en ocasiones, una actuación positiva por parte del Estado, en el sentido de promover las condiciones reales para la efectiva realización, como debe suceder con la identidad y la firma electrónica, presupuesto lógico para la actuación del ciudadano en la Red.

Como consecuencia ineludible de lo anterior, es posible afirmar que para el establecimiento de relaciones electrónicas tanto entre la Administración y el administrado, como entre diferentes Administraciones, e incluso en las relaciones internas de una misma Administración, resulta imperiosa la necesidad de emplear los instrumentos adecuados que garanticen circunstancias como la identidad del actor y la integridad y autenticidad de los datos y documentos. De no ser así, sería imposible la construcción de un entorno de confianza en el cual los actores puedan interactuar, y se frustran los beneficios de la digitalización de los trámites y procedimientos administrativos.

De hecho, una de las limitaciones más relevantes a las que se enfrentan hoy las redes de comunicaciones electrónicas de acceso público (y, en concreto, Internet) es la dificultad que existe a la hora de determinar a qué sitio Web nos conectamos y si dicho sitio al cual nos conectamos es o no seguro; y en sentido contrario, la dificultad para los titulares de sitios Web de determinar quién se conecta y con qué medidas de seguridad. En ese sentido, la falta de existencia de identidad en la red constituye, sin duda, una gran amenaza y una gran oportunidad para la comisión de infracciones civiles, administrativas, laborales e, incluso, actos delictivos[9].

Mecanismos de seguridad como la firma electrónica[10], al posibilitar la autenticación de una persona previamente identificada y la autenticación del origen de unos datos, contribuyen de forma decisiva a la necesaria creación de espacios de confianza, donde las partes, debidamente identificadas, generan documentos con valor probatorio pleno, que permiten – no sin retos importantes - la traslación a electrónico del tradicional expediente en papel.

En España resulta posible afirmar que en la actualidad contamos con dos leyes sobre firma electrónica. La primera, la Ley 59/2003, de 19 de diciembre, de firma electrónica, la cual constituye la transposición de la Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica y, la segunda, la propia LAECSP[11].

En la primera de las leyes es posible constatar la inclinación que tuvo el legislador por favorecer y fomentar el uso de la firma electrónica reconocida, como el paradigma de la seguridad y la confianza en Internet. De este modo, se establece el marco normativo en cuanto a los efectos que tienen los distintos tipos de firma electrónica, siendo la firma electrónica reconocida la única equivalente a la firma manuscrita y usable sin que sea necesaria la existencia de una norma jurídica que dé cobertura a su uso, aunque sin el "derecho a utilizarla". En otras palabras, la firma electrónica avanzada y la ordinaria necesitarían de una disposición normativa que habilite su uso en un entorno concreto, sin que el ciudadano pueda, además, exigir el uso de una identidad o firma electrónica concreta, quedando sujeto, por tanto, a la disposición de los medios que el proveedor (público o privado) considere necesarios[12].

Por su parte, la LAECSP crea nuevos tipos de firma electrónica, específicos para la Administración, y opta, en cuanto al uso de la firma electrónica – tanto de la Administración como de los ciudadanos – por un modelo de seguridad multinivel, ya que establece la posibilidad de empleo de los diversos mecanismos de autenticación y firma electrónica (ordinaria, avanzada o reconocida) en función del análisis de riesgo realizado por cada Administración Pública, dentro del marco de los principios de seguridad y proporcionalidad[13], y de los derechos a la obtención de la identidad electrónica y al empleo de la firma electrónica admitida por las Administraciones Públicas.

La mencionada LAECSP, sumamente consciente de la importancia de la necesidad de seguridad[14], dedica varios de sus artículos al desarrollo del tema de la identificación, la autenticación y la firma electrónica, tanto por parte de los ciudadanos como por parte de las propias Administraciones Públicas (personal al servicio de las Administraciones Públicas, sede electrónica[15], sello de órgano[16]). Y aunque el aludido marco multinivel pueda ser, en general, aplicable respecto de la identificación, autenticación y firma de las Administraciones Públicas, la LAECSP considera necesario en algunos casos, como el intercambio de datos entre Administraciones Públicas, se acuda a mecanismos que ofrezcan los máximos grados de seguridad.

El análisis combinado de ambas leyes – la ley general de firma electrónica y la ley especial, común en Derecho administrativo español, de identidad y firma electrónica en el sector público – conduce a un modelo en el que necesariamente han de existir diferentes sistemas y mecanismos de identidad y firma, como hemos visto: contraseñas estáticas, contraseñas dinámicas, mecanismos de segundo factor de autenticación, certificados en soporte software, certificados en soporte hardware, biometría…

Sistemas que, además, coexisten en el webespacio de aplicaciones y servicios informacionales interconectados, con los consiguientes retos para su funcionamiento

conjunto e interoperable, y sobre la base de la obligación legal para las Administraciones Públicas de aceptarlos, siempre que resulten adecuados en los términos planteados.

A partir de esta constatación, se han planteado diversas soluciones para la gestión de la identidad, entre las que destaca la propuesta de implementación de un metasistema de identidad, como manera de establecer a qué nos conectamos realmente. Este concepto puede materializarse mediante el establecimiento de mecanismos diversos, como los servicios web (web services), los cuales se erigen como una herramienta a través de la cual pueden construirse sistemas robustos y flexibles capaces de proporcionar recursos de distinta naturaleza que puedan evolucionar de acuerdo con el entorno[17].

La gestión interoperable de la identidad es una de las cinco prioridades máximas del programa de Administración electrónica de la Unión Europea, recogido en la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, «Plan de acción sobre Administración electrónica i2010: Acelerar la Administración electrónica en Europa en beneficio de todos», COM (2006) 173, de 25 de abril de 2006, que recoge y evoluciona el importante Acuerdo Signposts, adoptado a partir de la Declaración de Manchester de 2005.

Los principios aplicables a la gestión interoperable de la identidad deben ser los siguientes:

1. Usabilidad: las consideraciones de usabilidad deberán ser las más importantes en la creación del marco de trabajo europeo de gestión de identidad, que significa que el sistema debe ser seguro, implementar las salvaguardas necesarias para proteger la privacidad del usuario y permitir el uso de acuerdo con los intereses y las sensibilidades domésticas.

2. Identificación fuera de línea: cada Estado miembro debería ser capaz de identificar a los usuarios dentro de sus fronteras, si desea que disfruten del acceso a servicios de gestión de identidad que estén en el extranjero. Para conseguir este objetivo, hace falta emplear identificadores adecuados de manera consistente que permitan la identificación y la autenticación precisas de los usuarios, así como el intercambio de información entre las Administraciones Públicas en la medida necesaria para estos objetivos. Los requisitos fundamentales para un sistema que satisfaga las necesidades de las personas físicas que debería ser ampliable a personas jurídicas.

3. Identificación en línea: cada Estado miembro tendría que emitir los mecanismos necesarios a sus usuarios, para que éstos puedan identificarse y autenticarse electrónicamente, como condición para tener acceso a servicios de gestión de identidad cuando estén en el extranjero. El usuario debe tener la capacidad de actuar de manera autónoma y de hacer uso de los servicios ofrecidos.

4. Apoderamientos y autorizaciones: cada Estado miembro debería ofrecer los mecanismos para gestionar las competencias y capacidades de los usuarios

identificados dentro de sus fronteras, siempre que estas autorizaciones no se encuentren legalmente sujetas a aprobación por las autoridades de otro Estado miembro.

5. Validación en línea: cada Estado miembro tendría que ofrecer servicios en línea de validación de las identidades, competencias y autorizaciones, si desea ofrecer servicios de gestión de identidad.

6. Consenso: hay que establecer un consenso de alto nivel entre los Estados miembro sobre la terminología de gestión de identidad para garantizar la interoperabilidad conceptual y semántica, consenso que se podría confirmar mediante medidas políticas y legales apropiadas.

A partir de estos principios básicos se derivan una serie de criterios de diseño para el sistema europeo de gestión de identidad, con una orientación muy clara de la interoperabilidad del sistema, que debería:

1. Ser federado en un sentido político, por ejemplo, permitiendo a las Administraciones Públicas confiar mutuamente en los métodos de identificación y autenticación empleados, aceptándolos en la jurisdicción en la que se lleva a cabo el procedimiento siempre que también sean aceptables en el Estado de origen.

2. Ser multinivel, en el sentido de que los Estados miembro deberían poder ofrecer múltiples niveles de seguridad para los servicios de gestión de identidad, de forma que los requisitos de autenticación para cada servicio de Administración electrónica puedan ser ajustados a las necesidades de seguridad de aquel servicio. Los Estados miembro son los que deciden a qué nivel quieren ofrecer los servicios de autenticación, y cuál es el nivel de autenticación que se necesita para cada servicio, aunque han de aceptar como válido cualquier método de autenticación de este nivel suministrado por el resto de los Estados miembro. Esto implica definir un conjunto de criterios a escala europea para cada nivel de autenticación.

3. Confiar en fuentes de información auténtica. Para garantizar la calidad de los datos y la eficiencia de la Administración electrónica, tendría que existir al menos una fuente única y auténtica para cada punto de información de cada entidad registrada en el Estado miembro de origen, que puede ser una base de datos o un token (como un certificado).

4. Permitir una aproximación basada en sectores o contextos diferentes, cuando esto sea deseable para el Estado miembro de origen, y que de hecho supone una extensión lógica del modelo federado.

5. Permitir el desarrollo del mercado privado, en los casos en que los estados miembros decidan confiar en socios del sector privado (como por ejemplo entidades financieras) para la provisión de servicios de gestión de identidad a los usuarios.

La privacidad actúa como límite de especial relevancia en relación con los sistemas de identidad y de firma electrónica, por las consecuencias potenciales de la identificación masiva de las personas y la disposición de redes públicas que permiten el acceso a todas las bases de datos públicas con informaciones de estas personas.

Por este motivo, es especialmente importante que los citados sistemas de identidad y firma electrónica permitan la participación de las personas identificadas y, lo que es más importante, el control por parte de estas personas del acceso a los datos y la autorización para el intercambio en línea de sus datos, siempre de acuerdo con los estándares legalmente determinados de acuerdo con la legislación aplicable, hecho que también comporta un reto adicional en las relaciones con el elemento internacional.

III. El intercambio de información y la protección de datos de carácter personal

Otra de las grandes novedades legislativas introducidas por la LAECSP es, sin duda, el artículo 6.2.b), encargado de consagrar el derecho que tiene el ciudadano: "a no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizaran medios electrónicos para recabar dicha información siempre que, en el caso de los 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 (…)".

La consagración de este derecho no tiene precedentes en nuestro ordenamiento jurídico y, aunque su reconocimiento es fundamental para el funcionamiento de la Administración electrónica, tanto a partir del redactado de la norma como a partir del modelo elegido para su implementación, es posible que se planteen dudas acerca de una eventual colisión con el derecho fundamental de protección de datos personales.

En el entorno comunitario encontramos la Directiva 95/46/CE del Parlamento Europeo, sobre la protección de las personas físicas en lo que respecta al Tratamiento de Datos Personales y libre circulación, cuya transposición corresponde en nuestro ordenamiento jurídico a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal (en adelante, LOPD).

La LOPD tiene por objeto garantizar y proteger, en cuanto al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, especialmente los derechos de honor e intimidad personal y familiar. La mencionada Ley se aplica a los datos de carácter personal soportados físicamente y susceptibles de ser tratados, tanto en el ámbito público como privado.

Anteriormente, la protección de datos personales se había vinculado tradicionalmente a los derechos fundamentales consagrados en el artículo 18.1 de la CE, es decir, a los derechos al honor y a la intimidad personal y familiar y a la propia imagen. De suerte que las limitaciones en el intercambio y la cesión de datos e información por parte de

las Administraciones Públicas, solía encontrar límite en el respeto a la intimidad, el honor y la propia imagen del sujeto sobre el que recaía el mencionado intercambio.

Sin embargo, la jurisprudencia del Tribunal Constitucional se ha consolidado en dirección a considerar el derecho a la protección de datos como un derecho distinto del derecho de intimidad y que goza de una entidad jurídica propia[18]. Este derecho con status de fundamental, supone una limitación a los poderes públicos y a los entes privados, en el sentido en que todo intercambio de datos y de información supondrá el cumplimiento de las garantías y limitaciones consagradas constitucional y legalmente. Estas garantías se materializan, según el Tribunal Constitucional (STC 254/1993) en el derecho a requerir el previo consentimiento del interesado para la cesión y uso de sus datos personales, el derecho a saber y a ser informado sobre el uso y el destino de esos datos y el derecho a acceder, rectificar y cancelar dichos datos.

De otro lado, retomando el análisis de la LAECSP, el artículo 9 plantea las bases para la realización del derecho del ciudadano a no aportar datos que obren en poder de las Administraciones Públicas. Así, se dispone que estas deberán facilitar el acceso de las restantes (Administraciones) a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico[19], 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 acuerdo con lo establecido en la LOPD.

El segundo apartado establece que la disponibilidad de la que se habla se limita a los datos estrictamente requeridos por los ciudadanos para la actuación, tramitación y resolución de procedimientos de su competencia.

En este sentido, consideramos que la consagración de un modelo de confianza excesivamente laxo en favor de la Administración requirente del dato podría resultar, en la práctica, vulnerador del principio de proporcionalidad. En otras palabras, la no existencia de un requisito conforme el cual se requiera de una prueba robusta que acredite que efectivamente el ciudadano ha consentido en la cesión que se pretende llevar a cabo, puede infringir el derecho a la autodeterminación informativa del ciudadano, ya que permite el fraude interno y el acceso y divulgación no autorizada de información personal.

Esto es posible porque en su actuar las diferentes Administraciones pueden, eventualmente, efectuar peticiones de datos sin que efectivamente exista el consentimiento del ciudadano. Así, dado que la citada norma no establece un régimen estricto de control de datos por el ciudadano, consideramos determinante la implantación de un modelo garantista y seguro en la implementación del intercambio de datos que contrarreste las carencias legislativas.

Antes de pasar a hacer un breve análisis de los posibles modelos, resulta relevante mencionar que la LAECSP (en el artículo 42) crea el Esquema Nacional Interoperabilidad y el Esquema Nacional de Seguridad. Este último tendrá por objeto el establecimiento de la política de seguridad en la utilización de los medios

electrónicos, así como de los requisitos mínimos que permitan una protección adecuada de la información.

Es a estos Esquemas entonces a quienes corresponderá fijar los criterios y estándares que habrán de seguirse para que el intercambio de datos se lleve a cabo respetando los derechos fundamentales del administrado y, más concretamente, el respeto al derecho fundamental a la protección de datos.

IV. Modelos de implementación del intercambio de datos

1. Modelo basado en certificados telemáticos

El primer modelo objeto de análisis se construye a partir del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados.

Más concretamente, el artículo 13 autoriza la posibilidad de sustituir los certificados administrativos en soporte papel por certificados telemáticos, siempre que el interesado así lo autorice o una norma de rango legal lo disponga. Más adelante, el artículo 14 establece que el certificado telemático deberá contener los datos objeto de certificación y la firma electrónica de la autoridad competente para expedirlos. Dicho certificado pondrá ser expedido en atención a una solicitud hecha por el interesado o a instancia del órgano requirente (caso en el cual se debe contar con el consentimiento del interesado) y será enviado o puesto a disposición para su remisión al órgano que lo requiere.

Y es justamente en este punto en el que se plantea una de las debilidades del modelo: la Administración que expide el certificado telemático lo pone a disposición del administrado, y es el mismo quien debe transmitirlo a la Administración que requiere el dato. En este sentido el administrado tendría toda soportar la carga de transmitir documentos de Administración a Administración cada vez que lo necesitara.

Esta situación es francamente incompatible con las implicaciones que tiene la implantación de las nuevas tecnologías en la relación Administración-administrado, ya que éstas se erigen precisamente como herramientas que deben redundar en la mejora de la posición del ciudadano, en la medida en que le sean facilitados los medios para una mayor y mejor interacción y, desde luego, menor molestia en forma de cargas administrativas.

Por último, el modelo plantea problemas en cuanto a la interoperabilidad, ya que para su correcto funcionamiento todas las Administraciones Públicas debería pactar la homogenización absoluta de los formatos de los certificados telemáticos, cuestión, por supuesto, de más que difícil materialización en términos prácticos.

2. Modelo basado en transmisiones de datos entre Administraciones Públicas

El presente modelo surge precisamente con la finalidad de superar la principal debilidad del modelo de certificados telemáticos. En ese sentido, es posible afirmar que el presente modelo logra avanzar, al menos, en el hecho de liberar al administrado de la carga de trabajar para las Administraciones. Sin embargo plantea problemas desde otras perspectivas, como se verá a continuación.

Si bien también las transmisiones de datos se regulan inicialmente en el RD 209/2003, su fundamentación legal se encuentra hoy en el artículo 9 de la LAECSP, analizado en líneas anteriores, y establece básicamente que cada Administración deberá conceder acceso a las restantes Administraciones a los datos del interesado, especificando los protocolos, las condiciones y el funcionamiento del sistema de intercambio de acuerdo con las máximas garantías de seguridad, integridad y disponibilidad.

Desde la perspectiva de la legitimación subjetiva para solicitar y obtener el acceso a los datos de un ciudadano, en este modelo sólo las Administraciones se encuentran legitimadas para ello, de forma que el administrado no actúa en el procedimiento de intercambio; al contrario, la actuación se establece entre dos Administraciones Públicas, que tratan al ciudadano como un objeto sobre el que se intercambian datos, y no como un actor.

En otras palabras, el ciudadano se encuentra inmerso en la lógica de actuación Administración-Administración, lo que se traduce en su poca capacidad de decisión y de gestión sobre sus propios datos. Pareciera entonces que el modelo hubiera sido creado para responder a las necesidades de acceso de las Administraciones a los datos de los ciudadanos, si bien se encuentra subordinado el acceso a la realización del derecho a no aportar dichos datos, con los posibles problemas de acceso no autorizado a los datos que hemos expuesto anteriormente. En concreto, y como ya hemos visto, el hecho de que la cesión del dato se base en la presunción de que la Administración requirente efectivamente cuenta con el consentimiento del administrado hace que puedan resultar vulnerados derechos como el derecho fundamental a la protección de datos personales.

El modelo que estamos analizando tampoco toma en consideración las necesidades de otros actores del mercado que precisan acceder de forma legítima a datos del ciudadano en poder de las Administraciones Públicas, o que pueden disponer de datos del ciudadano a que deban acceder dichas Administraciones Públicas, como pueden ser las empresas[20]. En este caso al ciudadano le correspondería tramitar la transmisión de datos a través del modelo de certificados telemáticos. En definitiva, frente a cualquier situación que desbordara la lógica Administración-Administración se debe involucionar, ineludiblemente, hacia el primer modelo planteado y asumir sus limitaciones.

De otro lado, una de las limitaciones del modelo viene dada por la autenticación (tanto del administrado como del personal al servicio de las Administraciones Públicas) ya que, en atención al criterio acogido por la LAECSP, cada Administración estará facultada para exigir distintos niveles de identificación (firma electrónica ordinaria, avanzada o reconocida), hecho que podría configurarse como un grave obstáculo para

la interoperabilidad y el reconocimiento mutuo, y que sólo parece posible resolver mediante la aplicación combinada de los Esquemas Nacionales de Interoperabilidad y Seguridad, y los convenios interadministrativos de intercambio de datos previstos en el artículo 20 de la LAECSP..

Por último, y no por ello menos importante, precisamente en defensa de la protección del derecho a la protección de datos de carácter personal, el presente modelo está pensado para dar respuesta a los procedimientos administrativos iniciados a instancia de parte, ya que, como hemos indicado reiteradamente, se exige el consentimiento del ciudadano, aunque no necesariamente se comprueba la realidad del mismo.

De esta manera los procedimientos iniciados de oficio no tendrían cabida en el modelo, ya que faltaría el consentimiento aportado por el interesado para la realización del intercambio de datos, a no ser que exista una ley que excepcione la necesidad de dicho consentimiento[21], o que se arbitren mecanismos para que el ciudadano pueda "consentir anticipadamente[22]".

3. Modelo basado en la autogestión de datos y consentimientos personales para la transmisión de datos

Dadas las limitaciones de los anteriores modelos, resulta necesario implantar un modelo adicional, en el que el ciudadano pueda actuar en la medida justa para cubrir las carencias identificadas, beneficiándose de las ventajas de la reducción de aportación de documentación electrónica, a la vez que autorizando cesiones adicionales de datos en los restantes casos.

En este modelo[23], alineado con las propuestas innovadoras de las redes sociales que subyacen al paradigma del Web 2.0[24], el ciudadano es un agente más del sistema, que actúa depositando sus identidades electrónicas, atribuciones electrónicas, consentimientos para la cesión de datos personales y otras instrucciones a las Administraciones Públicas, empresas y otras instituciones.

El ciudadano puede realizar las siguientes actuaciones:

1. Registrar sus diferentes identidades electrónicas, estableciendo perfiles de usuario, que le permiten identificarse de forma unificada y segura frente a diferentes Administraciones y empresas. Por ejemplo, puede enlazar su identidad de banca electrónica con su certificado de ciudadano, de forma que podría integrar procedimientos de autenticación SSO entre la banca electrónica y la Administración para hacer seguimiento del trámite de comunicación de número de cuenta bancaria.

2. Registrar atribuciones electrónicas, que le permiten actuar mediante roles de usuario o atributos concretos. Por ejemplo, puede registrar su condición de administrador único societario – obtenida del certificado de firma electrónica – y emplear dicha condición para acceder a una carpeta de empresa y realizar actos en nombre de la sociedad mercantil en cuestión.

3. Conceder y retirar autorizaciones para que terceros actúen en su nombre. Por ejemplo, el anterior administrador único puede autorizar a sus trabajadores para que realicen determinados actos en nombre de la empresa, sin necesidad de apoderamiento notarial.

4. Registrar instrucciones dirigidas a Administraciones Públicas y empresas. Por ejemplo, puede indicar al sistema que instruye a la Administración local para que le practique una bonificación del cincuenta por ciento en la cuota del Impuesto de Bienes Inmuebles por ser titular del Libro de Familia Numerosa, sin necesidad de que le exija iniciar el trámite a instancia de oficio.

5. Registrar consentimientos para actos futuros y para cesiones de datos entre Administraciones y entre Administraciones y empresas y, lo que es más importante, prohibiciones de cesiones de datos entre dichas entidades. En este caso se obtiene una protección reforzada en términos de protección de datos de carácter personal, en la medida en que es el ciudadano quien programa el sistema para que la Administración cedente del dato tenga certeza sobre su consentimiento y aprobación. Para que la Administración cedente realmente suministre el acceso al dato deberá comprobar en este registro personal del ciudadano que el mismo ha autorizado la cesión.

De otro lado, el modelo supera otra de las dificultades fundamentales que presentaba el anterior modelo: el ciudadano puede autorizar a empresas privadas para que accedan a sus datos, y a Administraciones Públicas para acceder a datos en poder de empresas, además de poder transportar los documentos electrónicamente mediante su depósito en la plataforma.

V. Conclusiones y perspectivas de futuro

Del análisis anteriormente presentado se puede concluir que, aunque en tiempos recientes se han producido avances importantes en cuanto al derecho a la identidad electrónica y al uso de la firma electrónica, y en su aplicación a las relaciones entre las Administraciones Públicas, y entre éstas y los ciudadanos, los modelos previstos en la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos resultan insuficientes para cubrir todas las necesidades derivadas de la comunicación electrónica, especialmente a la luz de las restricciones impuestas por la legislación de protección de datos personales.

Cabe, por ello, trabajar en nuevos modelos, que con base en la innovación jurídica, nos permitan convertir al ciudadano en actor del sistema, con base en el uso de su identidad y su firma electrónica, de forma que podamos obtener un sistema de comunicación electrónica holístico e interoperable, con base en las técnicas de gestión de identidad y de las redes sociales del Web 2.0.

[1] En palabras de Cotino: “Procede fijar la atención en lo que es el eje medular de la ley, el reconocimiento, y como derecho subjetivo del derecho a relacionarse con las Administraciones públicas utilizando medios electrónicos. El mismo se reconoce en el artículo 6.1 LAE (…) Como se ha adelantado en general, la formulación de este

derecho es tajante a través de una norma categórica, que ya contiene la condición de aplicación del derecho y no requiere de una interpretación sistemática para saber cuándo debe ser aplicada. El ciudadano tiene el derecho a relacionarse con la Administración para las diversas y tan amplias finalidades que luego se estudian, y esta relación podrá ser por "medios electrónicos" si aquél lo quiere". Eduardo Gamero, Julián Valero Torrijos (coordinadores). La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. Editorial Aranzadi, SA., 2008, p. 147 y ss.

[2] Sobre el particular y a título ilustrativo, la Ley 58/2003, de 17 de diciembre, General Tributaria, en su artículo 96.2 dice lo siguiente: "Cuando sea compatible con los medios técnicos de que disponga la Administración tributaria, los ciudadanos podrán relacionarse con ella para ejercer sus derechos y cumplir con sus obligaciones a través de técnicas y medios electrónicos, informáticos o telemáticos con las garantías y requisitos previstos para cada procedimiento" (letra cursiva añadida al texto). El citado artículo somete el uso de los medios electrónicos por parte del administrado a la condición de la compatibilidad con los medios técnicos de que dispone, en éste caso, la Administración tributaria. En éste sentido, al ciudadano no le asistía más que una simple posibilidad de relacionarse electrónicamente sin que se configurase una obligación, en sentido estricto, en cabeza de la Administración.

[3] Art. 6.1 de la LAECSP.

[4] Art. 6.2.g). de la LAECSP.

[5] Art. 6.2.h) de la LAECSP.

[6] Art. 6.2.b). de la LAECSP.

[7] Como es sabido, en España únicamente ostentan el carácter de fundamental los derechos consagrados en la Constitución entre los artículos 14 y 29.

[8] En este sentido, es importante recordar que el derecho fundamental a la igualdad no es un derecho autónomo, sino que su vulneración se presenta siempre a partir de la vulneración de otro derecho. De esta manera podemos afirmar con García Morillo que: "(…) no se viola la igualdad en abstracto, sino en relación con –esto es, en la regulación, ejecución o aplicación, ejercicio, etc.- el acceso a los cargos públicos, la libertad de residencia, el derecho al trabajo o la tutela judicial efectiva, por solo poner unos ejemplos. El derecho a la igualdad reviste, por ello, un carácter genérico, en la medida en que se proyecta sobre todas las relaciones jurídicas y, muy en particular, sobre las que se fraguan entre los ciudadanos y los poderes públicos." (letra negrilla añadida al texto). Luis López Guerra, Eduardo Espín y otros. Derecho Constitucional. Volumen I. El ordenamiento constitucional. Derechos y deberes de los ciudadanos. Editorial Tirant lo blanch, 2003, p. 180.

[9] En este sentido, los datos de los estudios más recientes relativos a la seguridad de Internet en España ponen de manifiesto cifras alarmantemente altas en cuanto a

ordenadores domésticos y de PIME infectados por algún tipo de programa maliciosa (malware), situándose en el 77%; o relativas al correo fraudulento producido desde identidades inexistentes o falseadas, alcanzando el 85%. INTECO. Estudio sobre seguridad y confianza en los hogares españoles. Tercera Oleada. León. 2008.

[10] Es importante tener en cuenta que "la firma electrónica es un concepto legal, neutral desde una perspectiva tecnológica, que da cobertura al uso de cualquier tecnología que permita obtener las mismas funciones, con técnicas electrónicas, informáticas y telemáticas, que la firma de documentos en soporte papel". (texto original en catalán). Ignacio Alamillo Domingo. Abc de la signatura electrònica. Generalitat de Catalunya. Departament de Governació i Administracions Públiques, 2005, p.177 y ss.

[11] En la misma línea que otros Estados de la Unión Europea, como por ejemplo Austria, Alemania, Italia, Portugal, Eslovenia o Turquía. IDABC. Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications. SIEMENS y TímeLex para la Comisión Europea. 2007.

[12] Por ejemplo, en una relación electrónica con la Banca, es la entidad financiera la que decide de forma unilateral el medio de identidad y de firma electrónica a emplear, imponiendo dichos medios a sus clientes por vía contractual.

[13] Los principios de proporcionalidad y de seguridad se encuentran consagrados en el artículo 4 de la LAECSP. El primero hace referencia a que la exigencia de un determinado nivel de acreditación debe circunscribirse a la naturaleza y circunstancias de los distintos trámites y procedimiento. Este principio actúa como límite superior, no pudiendo exigirse un nivel de seguridad más alto que el que resulta adecuado y necesario en el procedimiento tradicional basado en soporte papel. El segundo, establece que en el escenario telemático se exigirán al menos el mismo nivel de garantías exigidas en los trámites y procedimientos llevados a cabo por los conductos tradicionales. Este principio actúa como límite inferior, garantizando un tratamiento equivalente en términos de seguridad a los diferentes canales de tramitación (en soporte papel y en soporte electrónico).

[14] Hasta el 60% del articulado legal contiene referencias a la seguridad de la información, en sus diferentes dimensiones (integridad, autenticidad, confidencialidad, disponibilidad).

[15] Según el artículo 10.1 de la LAECSP: "La sede electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias". En cuanto a la Identificación de las sedes electrónicas el artículo 17 establece que utilizaran "sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente".

[16] En los términos establecidos por el artículo 18 de la LAECSP, el sello electrónico de Administración Pública, órgano o entidad de derecho público sirve para la identificación y autenticación del ejercicio de la competencia en la actuación administrativa automatizada y debe basarse en un certificado electrónico de acuerdo con lo establecido en la legislación sobre firma electrónica.

[17] Kim Cameron. The laws of identity. En: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[18] "Así, en sus SSTC 144/1999 (caso: "Los antecedentes penales de Hormaechea") y 292/2000 (caso: "Inconstitucionalidad de la LORTAD"), establece con relación al primero, que la función del derecho a la intimidad es la de proteger cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar, que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. Por el contrario, el derecho a la protección de datos persigue garantizar a la misma persona un poder de control sobre sus datos personales, sobre su uso y sobre el destino que les está atribuido, al objeto de evitar un tráfico ilícito y lesivo de la dignidad y del derecho del afectado" Citado en: Marc Carrillo. El Derecho a no ser Molestado. Editorial Aranzadi, 2003, p.95.

[19] Nótese que no resulta exigible pasar los datos que se encuentren en soporte papel a forma electrónica, por lo que, en estos casos, la inacción de la Administración resulta suficiente para que el derecho del ciudadano sea vea limitado.

[20] Nótese que ni siquiera las empresas públicas están legitimadas para ello.

[21] Es importante resaltar que con base en la LAECSP, la única posibilidad que tienen las Administraciones Públicas de iniciar un procedimiento de oficio es la establecida en el artículo 27.6, según el cual se podrá establecer reglamentariamente la obligatoriedad de la relación electrónica cuando los interesados se correspondan con personas o colectivos a los cuales pueda presuponérsele su capacidad de acceso a los medios electrónicos.

[22] Por ejemplo, en algunos casos la Administración capta el consentimiento para un acto futuro, como el envío de los datos fiscales para la campaña de la Renta del ejercicio siguiente, mientras que en otros se considera la "suscripción" del ciudadano a notificaciones de actos iniciados de oficio.

[23] El proyecto PASSI – Plataforma de Atributos de Seguridad y Firma Electrónica, de la Agència Catalana de Certificació es un ejemplo de implantación de este novedoso modelo.

[24] Como por ejemplo Facebook, donde el ciudadano carga sus informaciones y decide con quién y cómo las comparte, por citar sólo un ejemplo.

* Ignacio Alamillo: Abogado. Consultor senior en seguridad de la información (Dirección General de la Sociedad de la Información. Secretaría de Telecomunicaciones y Sociedad de la Información. Generalitat de Catalunya)
Licenciado en Derecho. Abogado del Ilustre Colegio de Madrid. Director del área de asesoramiento e investigación de la Agència Catalana de Certificació (diciembre 2002-febrero 2008). Director del área de consultoría y servicios legales de la Agencia de Certificación Electrónica – ACE (julio 1997-diciembre 2002). Miembro del grupo directivo europeo de Seguridad de Redes y de la Información y del grupo directivo de la Iniciativa Europea de Normalización de la Firma Electrónica, asesorando a la Comisión Europea. Miembro del Consejo de Certificación de ASIMELEC. Ha sido miembro del grupo directivo europeo de la Iniciativa Europea de Normalización de la Firma Electrónica, y del grupo de Infraestructura de Seguridad de Firma Electrónica del Instituto Europeo de Normas de Telecomunicaciones. Autor del “ABC de la firma electrónica”, coautor de cuatro libros sobre aspectos jurídicos de la sociedad de la información, numerosos artículos y ponencias en firma electrónica y su campo de aplicación.

Erika Henao Hoyos: Agència Catalana de Certificació

Disponível em: < http://www.alfa-redi.org/rdi-articulo.shtml?x=10736 > Acesso em: 22 set. 2008.